

Countering Attacks at Layer 2

Eric Smith
ejsmith@bucknell.edu

Shmoocon 2006

Who am I?

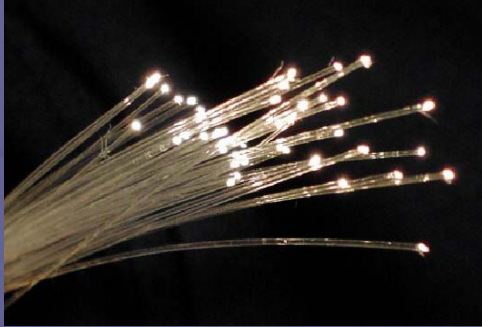
Network Administrator
Bucknell University
Lewisburg, PA

www.bucknell.edu



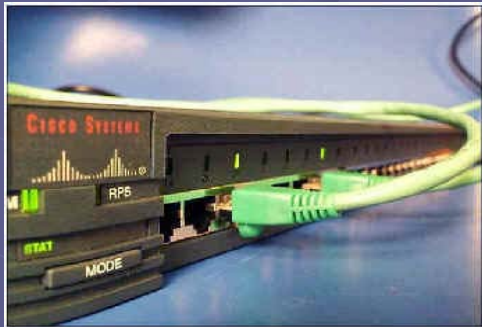
3,500 Students
450 Acre Campus
10k Node Ethernet Network
900 Network Devices (350 APs)
500 miles of fiber optic cable

What is Layer 2?



(1) Physical – Bits

Cat5, fiber, coax, aether



(2) Data-Link – Frames

Ethernet
switches and hubs



(3) Network – Packets

IP, IPX, Appletalk
routers, firewalls

The Layer 2 Utopia

- Layer 2 (Ethernet) protocols were written in friendlier, more trusting times



First Ethernet Standard: 1980

- Virtually no authentication, data is assumed by client machines to be valid



Must be in the same collision domain to exploit L2

Most firewalls don't care about L2 attacks

Most switches will assist in a L2 attack

The M&M Security Model



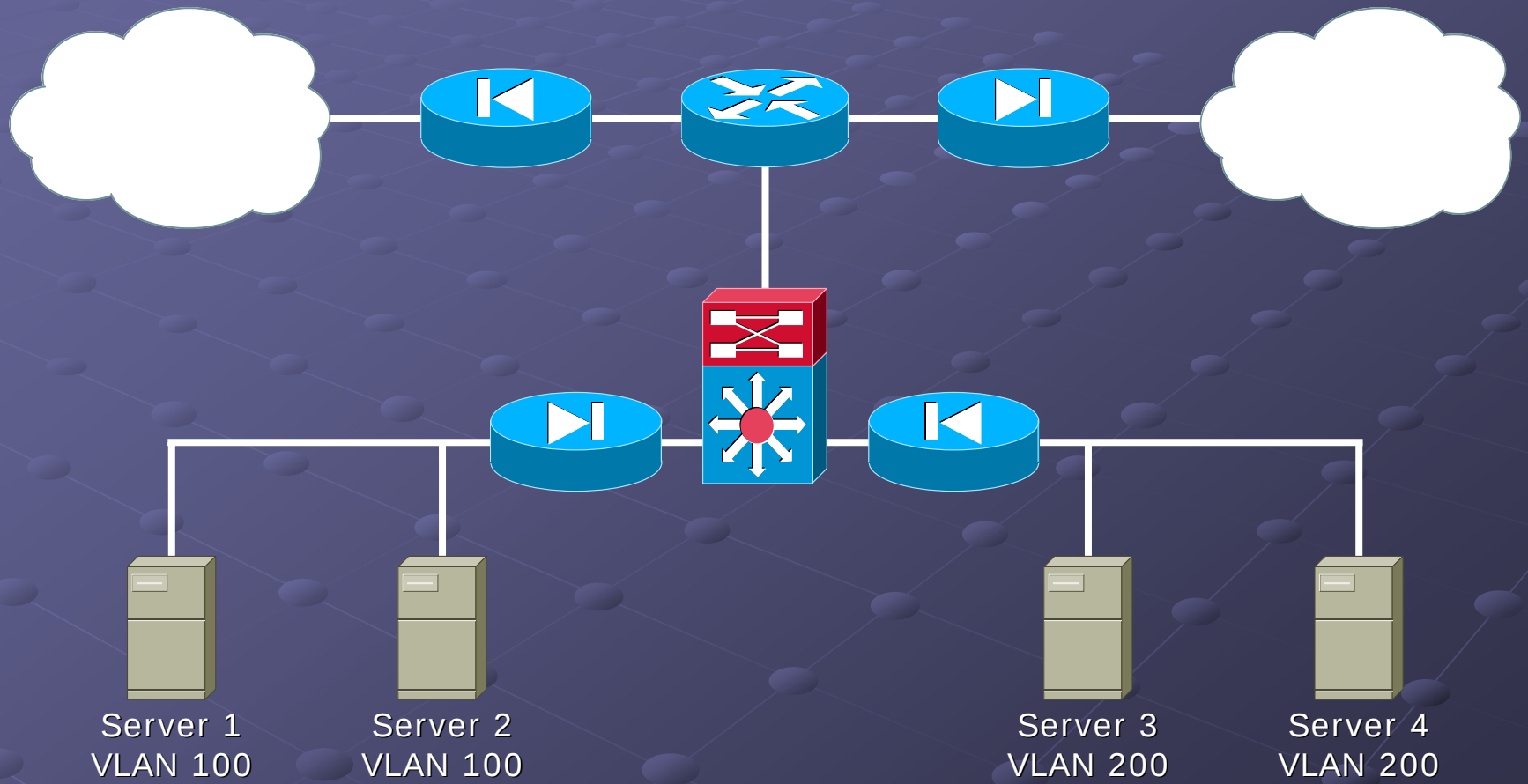
Hard and Crunchy on the Outside...

- Firewalls
- VPN / Crypto / SSL
- IDS / IPS

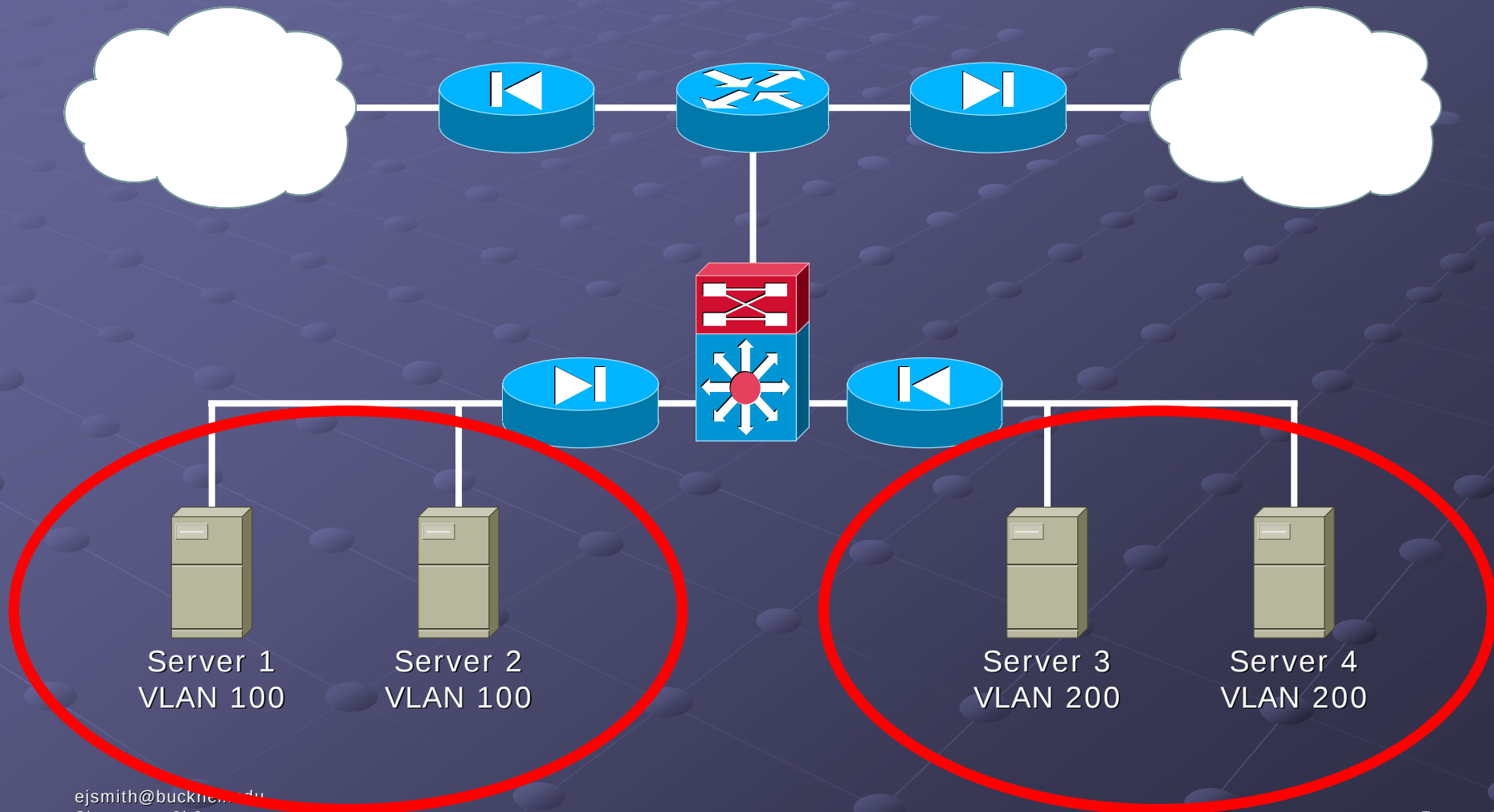
...Soft and Chewy on the Inside

- Unfirewalled hosts
- Vulnerable interior Services
- **Ethernet, Layer 2**

L2-Vulnerable Networks



L2-Vulnerable Networks



Am I vulnerable?

Does a potential attacker have L2 connectivity to your box?

Direct - universities (ResNet), most corporate LANs (co-workers), hotels, hotspots... especially those at security conferences... :)

Indirect – L3 takeover of L2 neighbor

If so... you are probably vulnerable.



Layer 2: Who Cares?

Networks where L3 Boundaries do not necessarily exist

➔ WiFi Hotspots, Hotels, Universities



Who cares.. I'm firewalled

L2Recon Demo

Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://presetkillimit.us/l2recon.html

Go

PreSet Kill Limit presents...
L2 Information Leakage
52 unique machines identified
presetkillimit.us



IP	MAC	Machine Name	Data Source
192.168.42.1	000a95f0504e Apple Computer, Inc.		IP Data
192.168.42.100	000a956d9448 Apple Computer, Inc.		ARP
>> ARP Request 192.168.42.100:000a956d9448 for 192.168.42.100:000000000000			
192.168.42.100	000a956d9448 Apple Computer, Inc.		ARP
>> ARP Request 192.168.42.100:000a956d9448 for 192.168.42.254:000000000000			
192.168.42.100	000a956d9448 Apple Computer, Inc.		IGMP Membership Report - 224.0.0.251
192.168.42.100	000a956d9448 Apple Computer, Inc.		IP Data
 192.168.42.101	00b0d0410f13 Dell Computer Corp.	ACCOUNTING __MSBROWSE__	SMB Browser (WIN)
 192.168.42.101	00b0d0410f13 Dell Computer Corp.	ACCOUNTING BUCKNELL	SMB Browser (WIN)
192.168.42.102	00145100955a Apple Computer Inc.		IGMP Membership Report - 224.0.0.251

Done

Adblock

Agenda



ARP

MAC Spoofing

Spanning Tree

Cisco Discovery Protocol (CDP)

Dynamic Trunking Protocol (DTP)

Broadcast Flooding

Putting it all Together

Attacks at L2: ARP

Ethernet Address Resolution Protocol – RFC 826

<http://www.faqs.org/rfcs/rfc826.html>

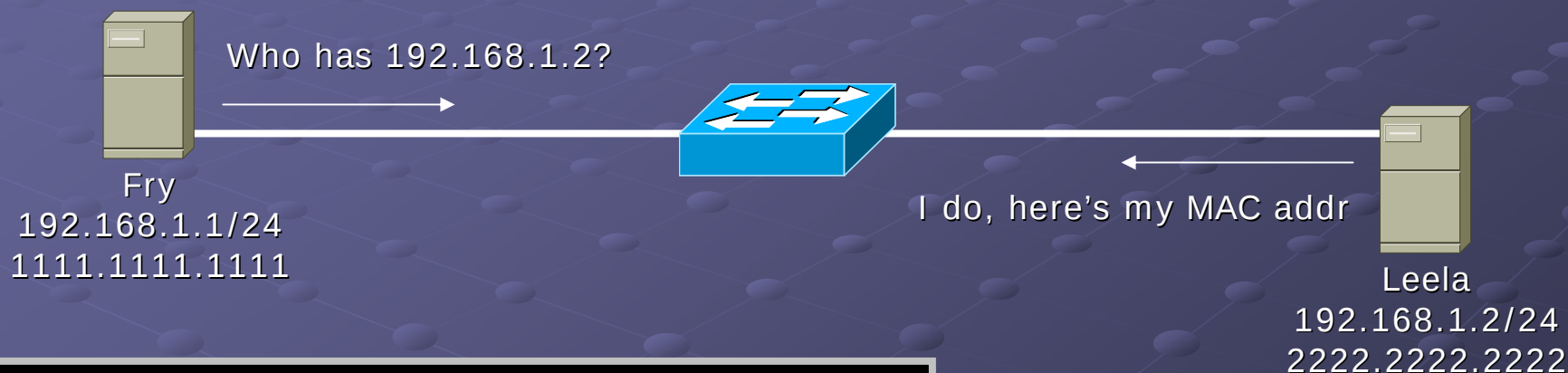
Defines the mapping of L2 address to a L3 Address

...Almost always done dynamically...



Attacks at L2: ARP

Fry wants to ping Leela...



```
C:\Fry>arp -a
```

```
Interface: 192.168.1.1 --- 0x2
```

Internet Address	Physical Address	Type
192.168.1.2	22-22-22-22-22-22	dynamic

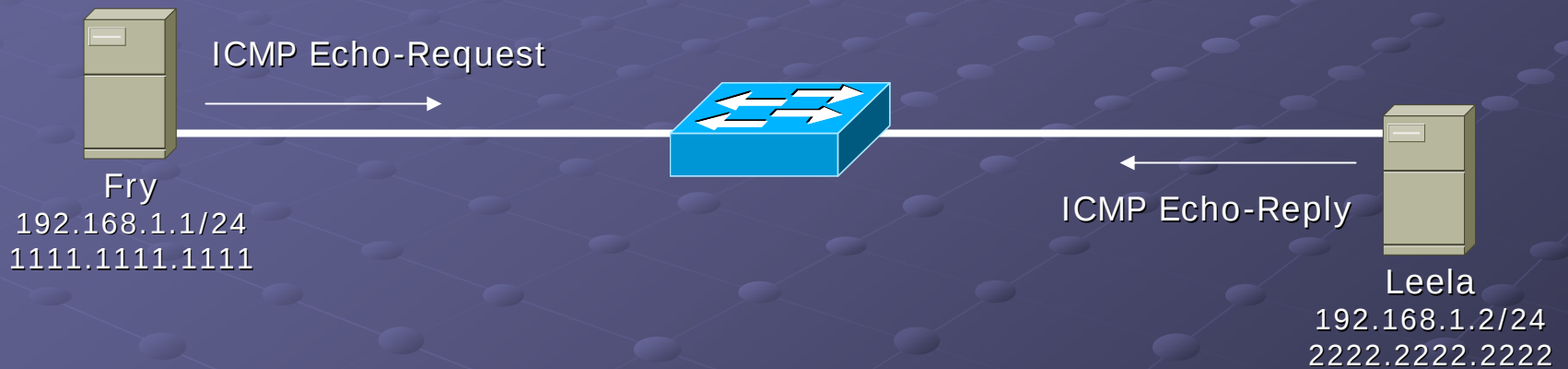
```
C:\Leela>arp -a
```

```
Interface: 192.168.1.2 --- 0x2
```

Internet Address	Physical Address	Type
192.168.1.1	11-11-11-11-11-11	dynamic

Attacks at L2: ARP

Fry wants to ping Leela...



2222.2222.2222	1111.1111.1111	0800	IP Header	IP Payload [ICMP]
----------------	----------------	------	-----------	-------------------

Attacks at L2: ARP

Enter the attacker...



Fry

192.168.1.1/24
1111.1111.1111



192.168.1.2 is at
3333.3333.3333



Leela

192.168.1.2/24
2222.2222.2222



Zapp

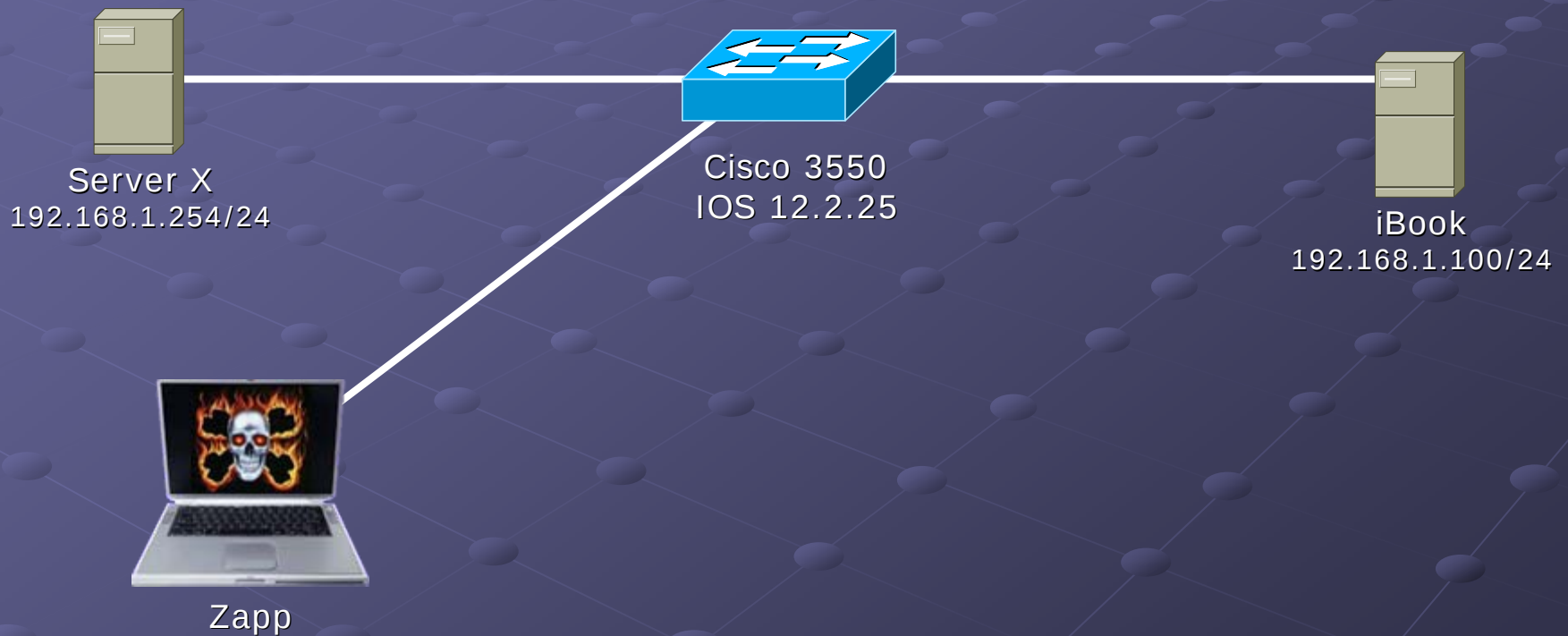
192.168.1.3/24
3333.3333.3333

```
C:\Fry>arp -a
```

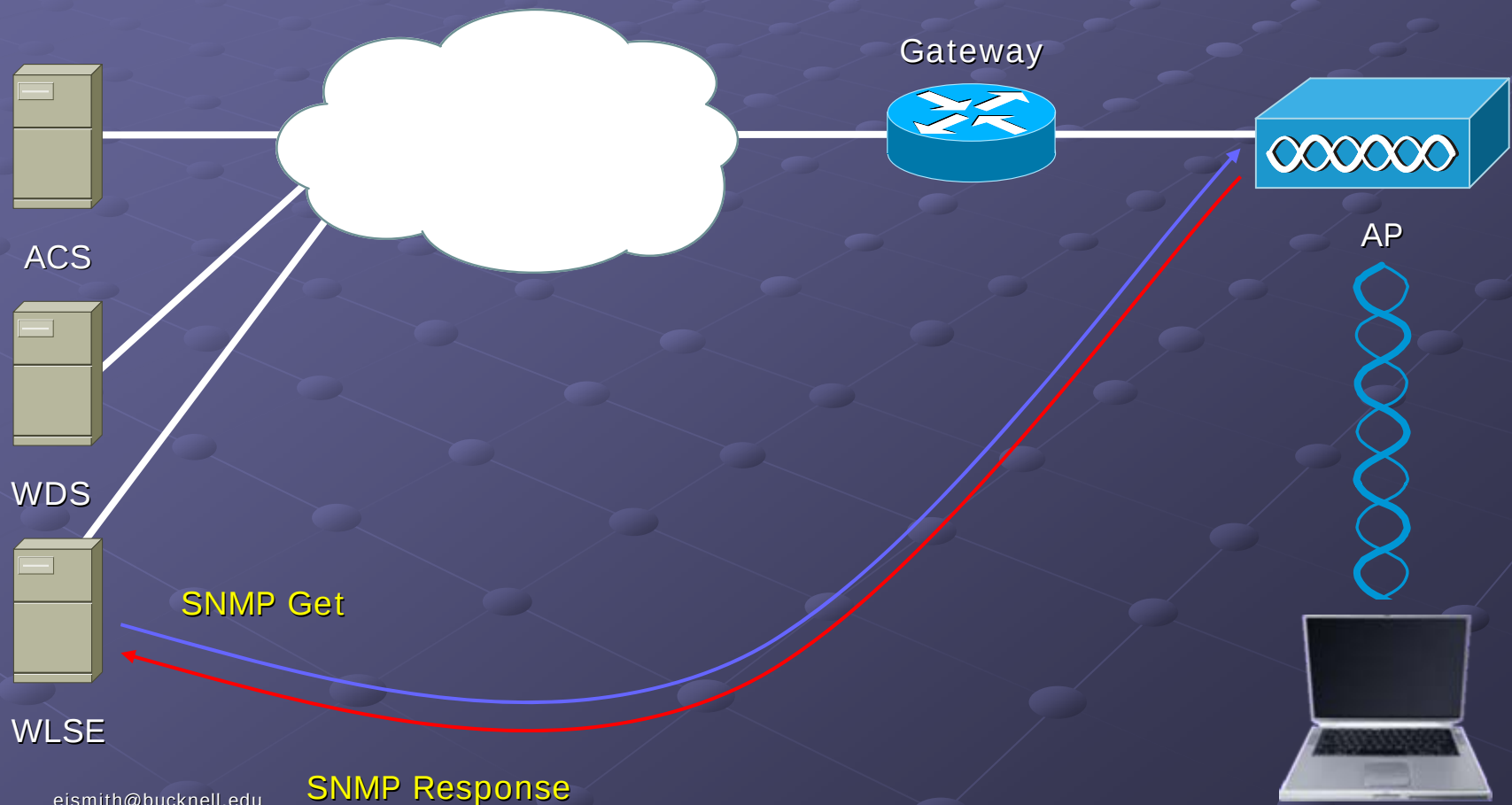
```
Interface: 192.168.1.1 --- 0x2
```

Internet Address	Physical Address	Type
192.168.1.2	33-33-33-33-33-33	dynamic

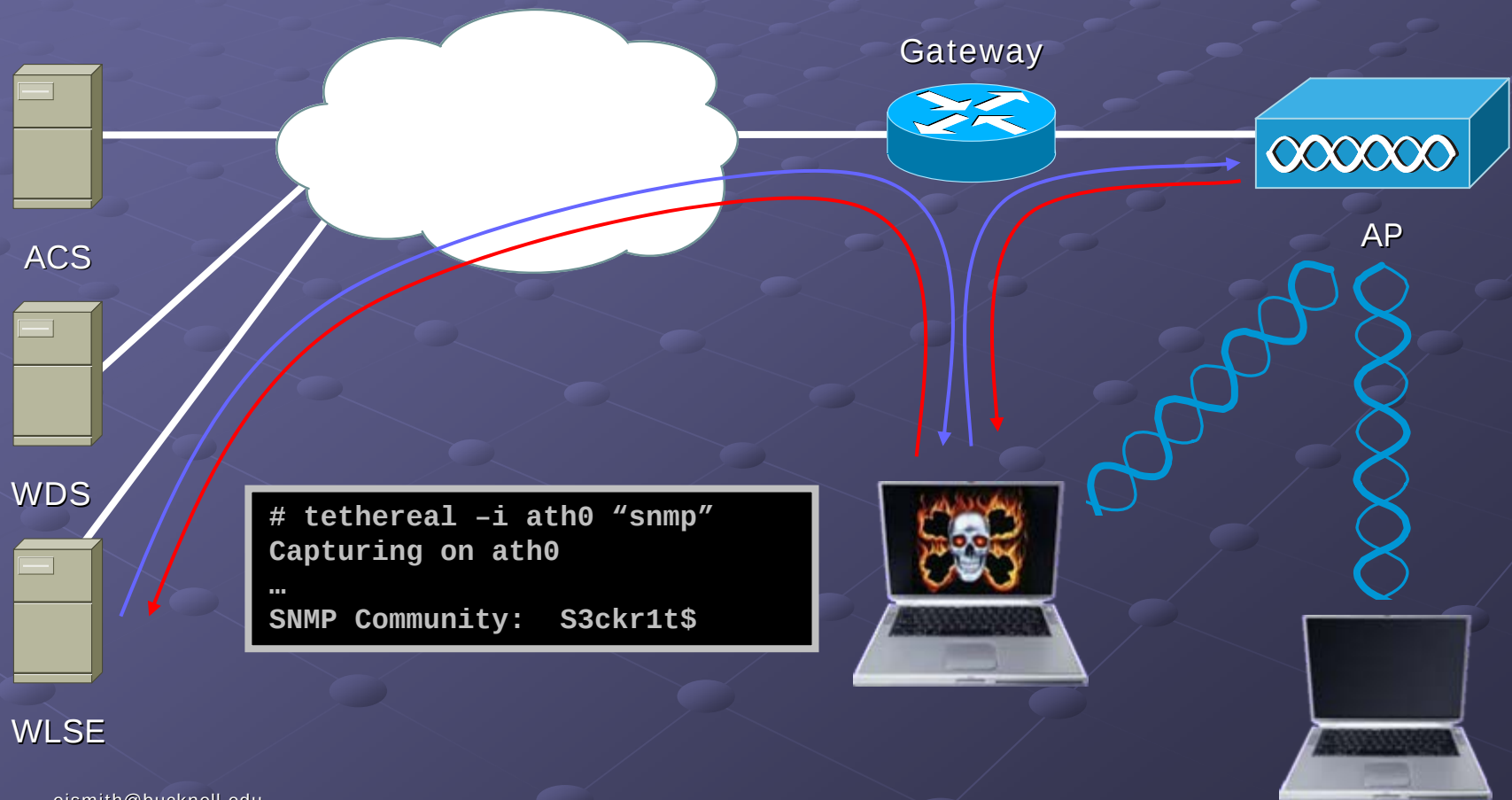
ARP Spoofing Demo



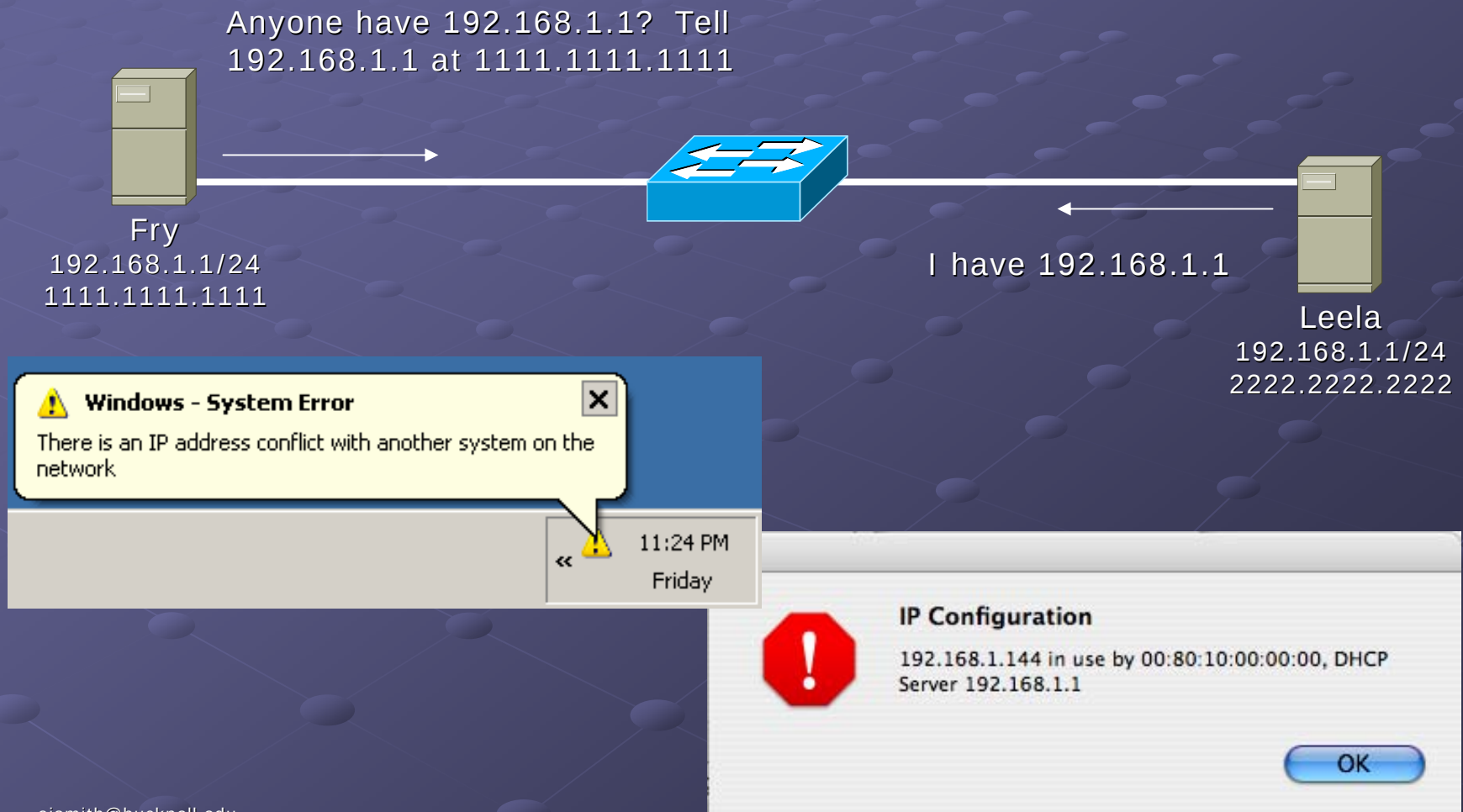
Cisco “Distributed” Wireless Infrastructure ARP Attacks



Cisco “Distributed” Wireless Infrastructure ARP Attacks

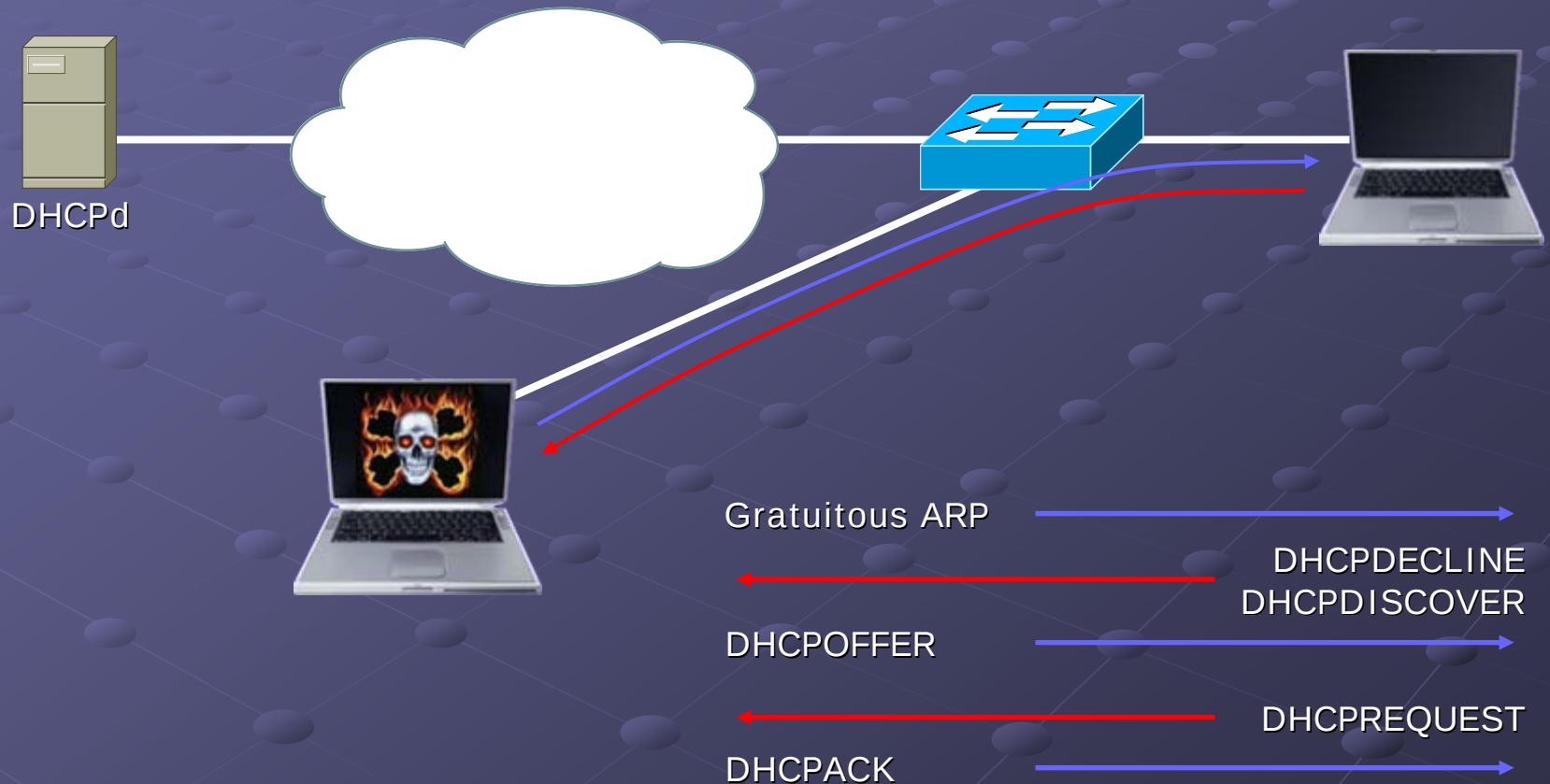


Gratuitous ARP Attacks



Gratuitous ARP Attacks

OSX Overreaction demo



Cisco ARPD 0-day DOS

cisco.com/warp/public/707/cisco-sa-20060112-wireless.shtml

Cisco BugID CSCsc16644

IOS < 12.3(7)JA1 are vulnerable

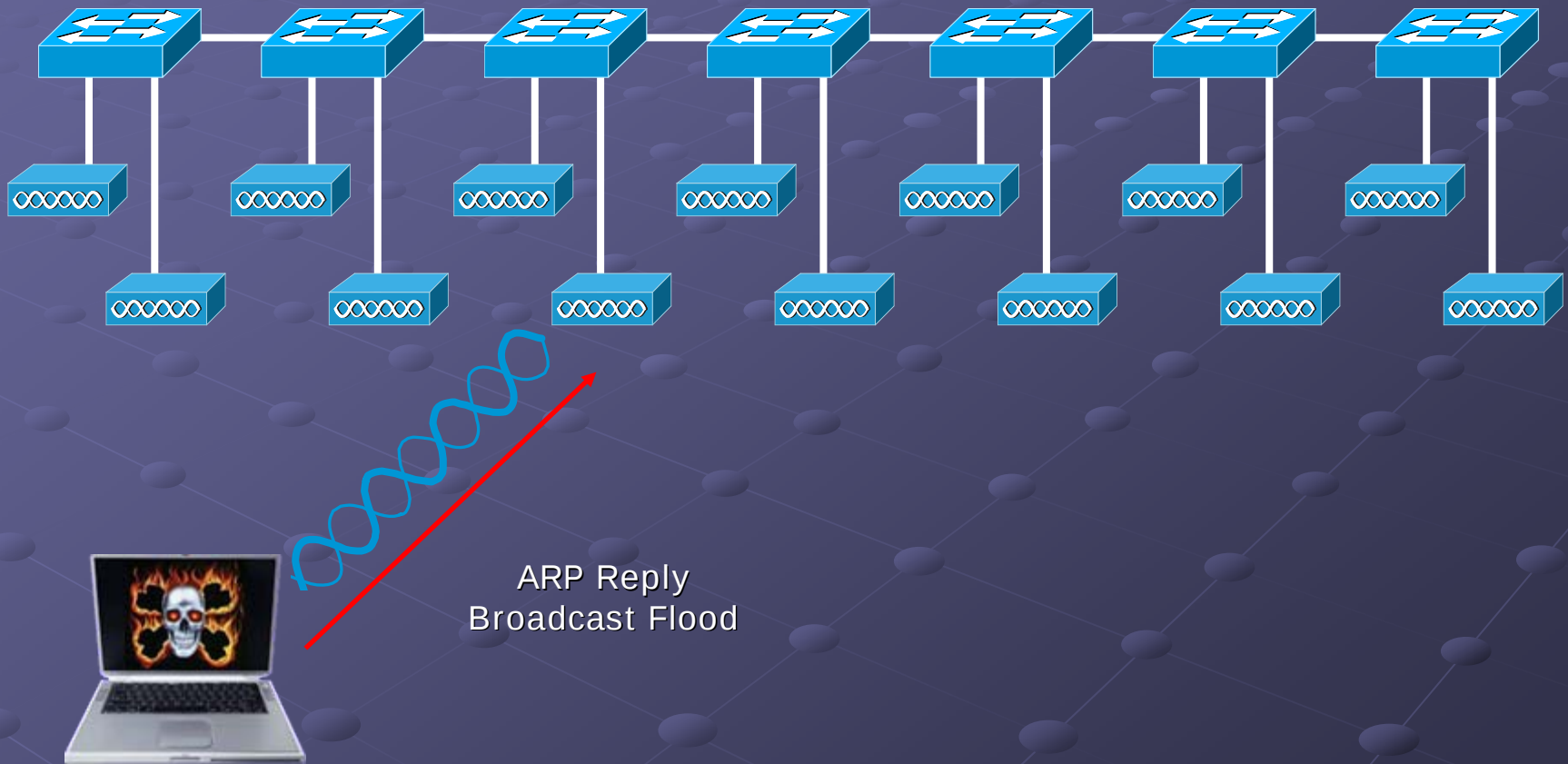
Affects most Cisco AP's:

1400	1300
1240AG	1230AG
1200	1130AG
1100	350



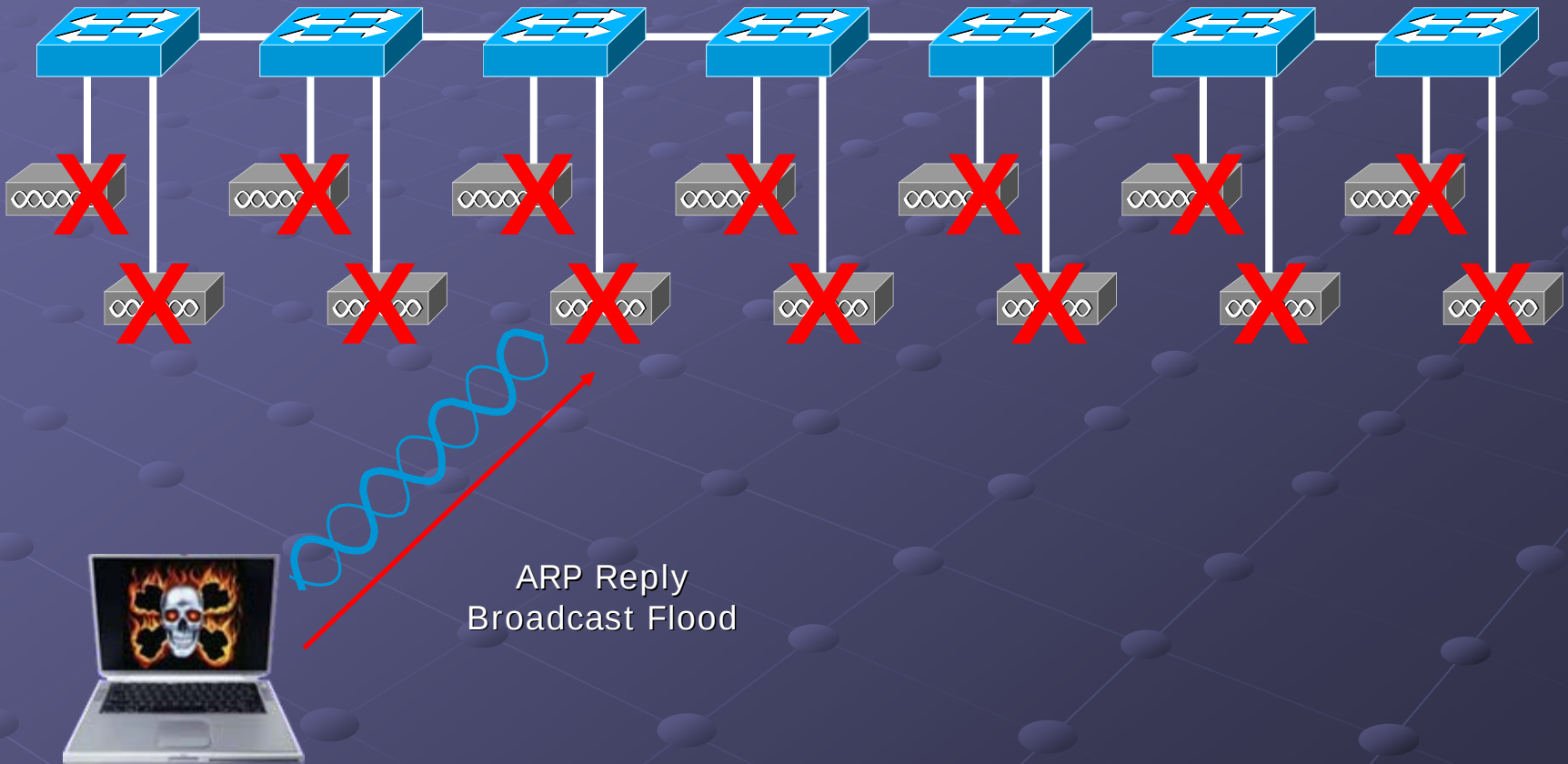
Cisco ARPD 0-day DOS

Bloomsburg University Field Test



Cisco ARPD 0-day DOS

Bloomsburg University Field Test



Cisco ARPD 0-day DOS

Wireless LAN Solution Engine - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://wireless.bloomu.edu:1741/main.html

email enc Library Mt MegaTokyo network PayPal PennyArcade PSECU Slashdot SquirrelMail - Login VG Cats - Comics WebCal KLN ENC

CISCO SYSTEMS **Wireless LAN Solution Engine** Wizard | Overview | Help | About | Logout Wed Jan 11, 2006 8:52:04

IDS Faults Devices Configure Firmware Reports Radio Mgr Sites Admin

Display Faults Manage Fault Settings Notification Settings

Filter Faults Products All Severity All State Active Name/IP Refresh(Sec) 300 Apply

Fault Summary

	Address	Name	Family	Product	Type	Description	Severity	State	Timestamp
☐	149.137.181.33	AL3-Zone3-AP3.bloomu.edu	Aironet	AP 1210	Device	Device was not reachable via SNMP	P1	Active	08:50:46 01/11/2006
☐	149.137.181.32	AL3-Zone2-AP2.bloomu.edu	Aironet	AP 1210	Device	Device was not reachable via SNMP	P1	Active	08:50:46 01/11/2006
☐	149.137.181.42	AL4-Zone2-AP2	Aironet	AP 1210	Device	Device was not reachable via SNMP	P1	Active	08:50:46 01/11/2006
☐	149.137.181.41	AL4-Zone1-AP1	Aironet	AP 1210	Device	Device was not reachable via SNMP	P1	Active	08:50:46 01/11/2006
☐	149.137.181.13	AL1-Zone3-AP3.bloomu.edu	Aironet	AP 1210	Device	Device was not reachable via SNMP	P1	Active	08:50:46 01/11/2006
☐	149.137.181.22	AL2-Zone2-AP2.bloomu.edu	Aironet	AP 1210	Device	Device was not reachable via SNMP	P1	Active	08:50:46 01/11/2006
☐	149.137.181.21	AL2-Zone1-AP1.bloomu.edu	Aironet	AP 1210	Device	Device was not reachable via SNMP	P1	Active	08:50:46 01/11/2006
☐	149.137.181.11	AL1-Zone1-AP1.bloomu.edu	Aironet	AP 1210	Device	Device was not reachable via SNMP	P1	Active	08:50:46 01/11/2006
☐	149.137.181.43	AL4-Zone3-AP3	Aironet	AP 1210	Device	Device was not reachable via SNMP	P1	Active	08:50:46 01/11/2006
☐	0013c32ed8b0	0013c32ed8b0	UnknownIEEE802dot11	Unknown AccessPoint	Unknown Station	Device state is switchport traced rogue access point	P1	Active	14:41:04 01/10/2006
☐	149.137.181.242	MCS-rm1154-B.bloomu.edu	Aironet	AP 1210	Device	Device was not reachable via SNMP, Inconsistent state found for query "interface.radio.config"	P1	Active	06:49:28 07/26/2005

Done

Cisco ARPd 0-day DOS

Bloomsburg University Field Test



ARP Countermeasures

1) Static ARP Assignments

Potential administrative nightmare (for you!)

```
cat6k-MSFC# sh run int vlan 123
```

```
interface Vlan123
  description Accounting
  mac-address 0000.0000.0123
  no arp arpa
  ip address 172.16.123.254 255.255.255.0
end
```

```
Cat6k-MSFC(config)# arp 172.16.123.1 2716.0570.0000
```

ARP Countermeasures

Static ARP assignments



Fry

192.168.1.1/24
1111.1111.1111



192.168.1.2 is at
3333.3333.3333



Leela

192.168.1.2/24
2222.2222.2222



Zapp

192.168.1.3/24
3333.3333.3333

```
C:\Fry>arp -s 192.168.1.2 22-22-22-22-22-22
```

```
Interface: 192.168.1.1 --- 0x2
```

Internet Address	Physical Address	Type
192.168.1.2	22-22-22-22-22-22	static

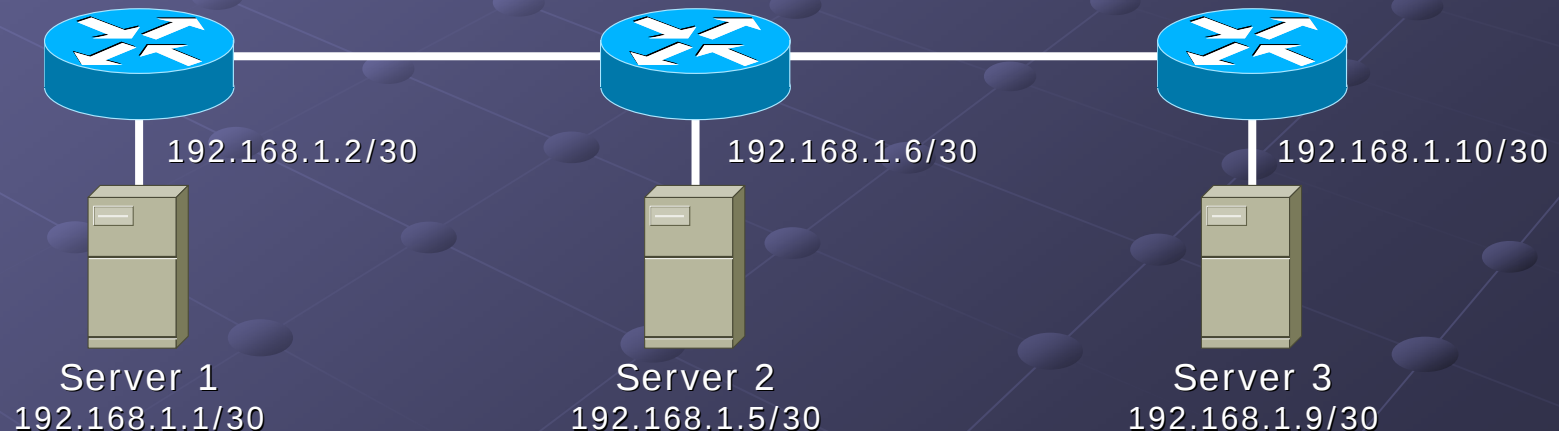
ARP Countermeasures

2) No L2 Neighbors

wastes a lot of IP space; numerous VLANs; difficult to scale

```
cat6k-MSFC# sh run int vlan 1000
```

```
interface Vlan1000
description Quake4 Server
ip address 192.168.1.2 255.255.255.252
end
```



ARP Countermeasures

3) IPSec/SSH/VPN/Etc

Accept L2 as weak and encrypt at higher levels

4) 802.1q Trunks

Never allow client machines to share VLAN space with your infrastructure equipment's management interfaces!

5) Private VLANs

6) Dynamic ARP Inspection (via DHCP Snooping Table)

7) Arpwatch (www-nrg.ee.lbl.gov)

***** Remember: 802.1x does not help! *****

Agenda

ARP



MAC Spoofing

Spanning Tree

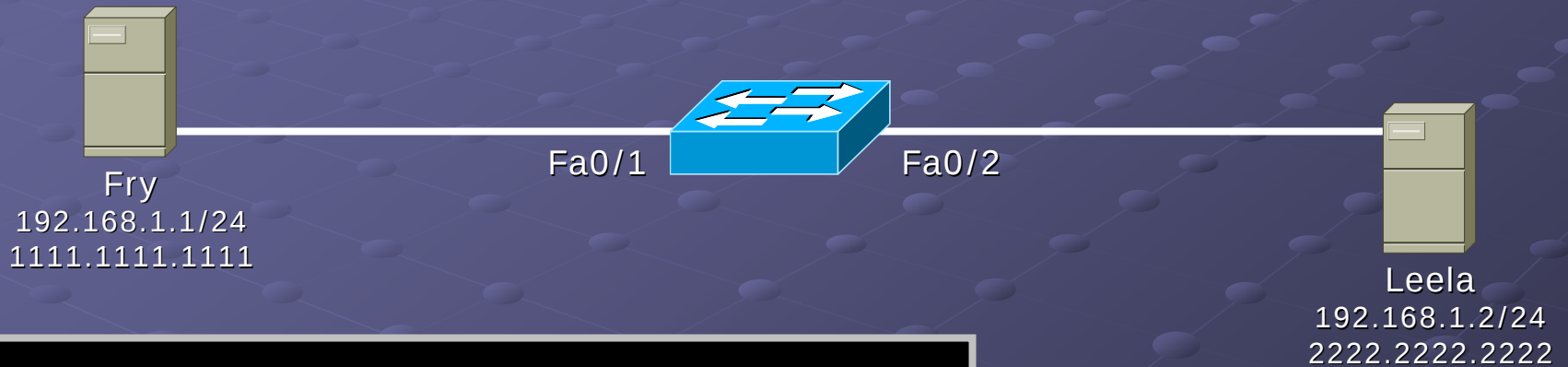
Cisco Discovery Protocol (CDP)

Dynamic Trunking Protocol (DTP)

Broadcast Flooding

Putting it all Together

MAC Spoofing Attacks

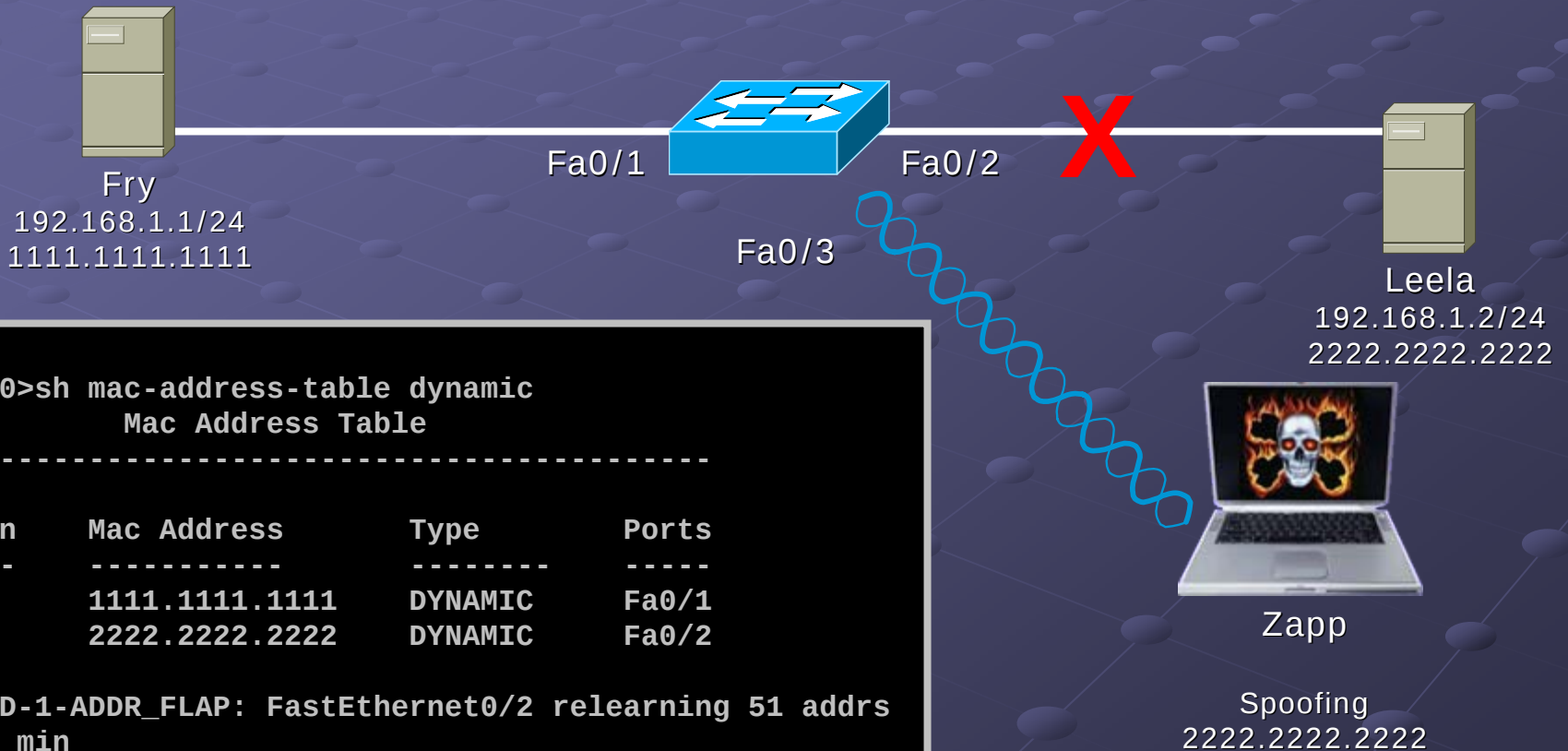


```
3550>sh mac-address-table dynamic
      Mac Address Table
```

Vlan	Mac Address	Type	Ports
1	1111.1111.1111	DYNAMIC	Fa0/1
1	2222.2222.2222	DYNAMIC	Fa0/2

MAC Spoofing Attacks

Enter the attacker...



MAC Spoofing Countermeasures

1) Port Security: Dynamic or Static

```
interface FastEthernet0/1
  desc 107B2 - Guest port in 1st floor conference room
  switchport mode access
  switchport port-security
  switchport port-security maximum 1
  switchport port-security violation { restrict | shutdown }
end
interface FastEthernet0/2
  desc 144B1 - Laser printer near public entrance
  switchport mode access
  switchport port-security
  switchport port-security maximum 1
  switchport port-security violation { restrict | shutdown }
  switchport port-security mac-address 2716.0570.0000
end
```


MAC Spoofing Countermeasures

2) Static MAC Address Assignments

```
3550(config)# mac-address-table static 0000.0000.0001  
vlan 10 interface FastEthernet0/1
```

```
3550#sh mac-address-table static interface fa0/1  
Mac Address Table
```

```
-----  
Vlan      Mac Address      Type      Ports  
----      -  
10        0000.0000.0001   STATIC    Fa0/1  
Total Mac Addresses for this criterion: 1
```

Agenda

ARP

MAC Spoofing



Spanning Tree

Cisco Discovery Protocol (CDP)

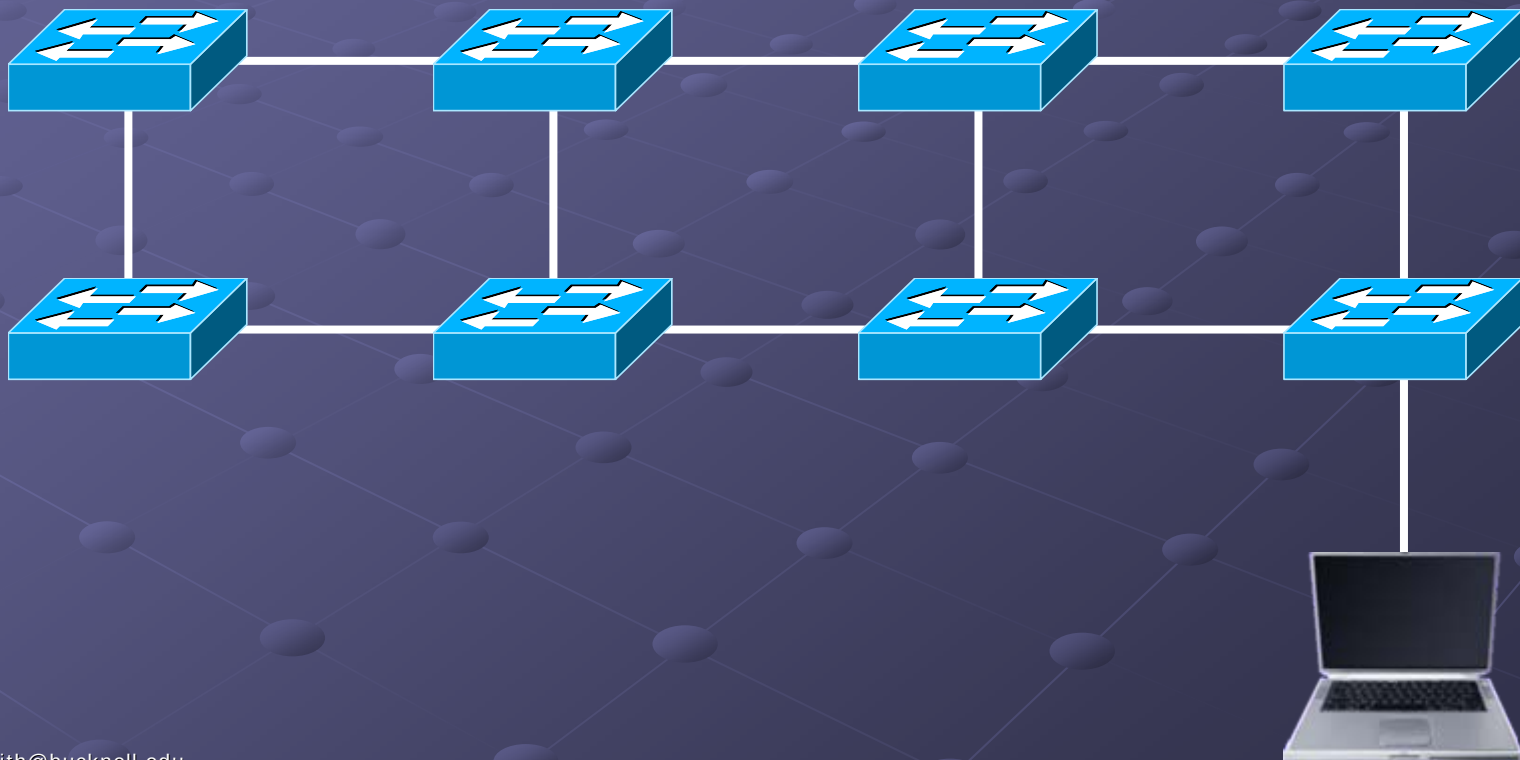
Dynamic Trunking Protocol (DTP)

Broadcast Flooding

Putting it all Together

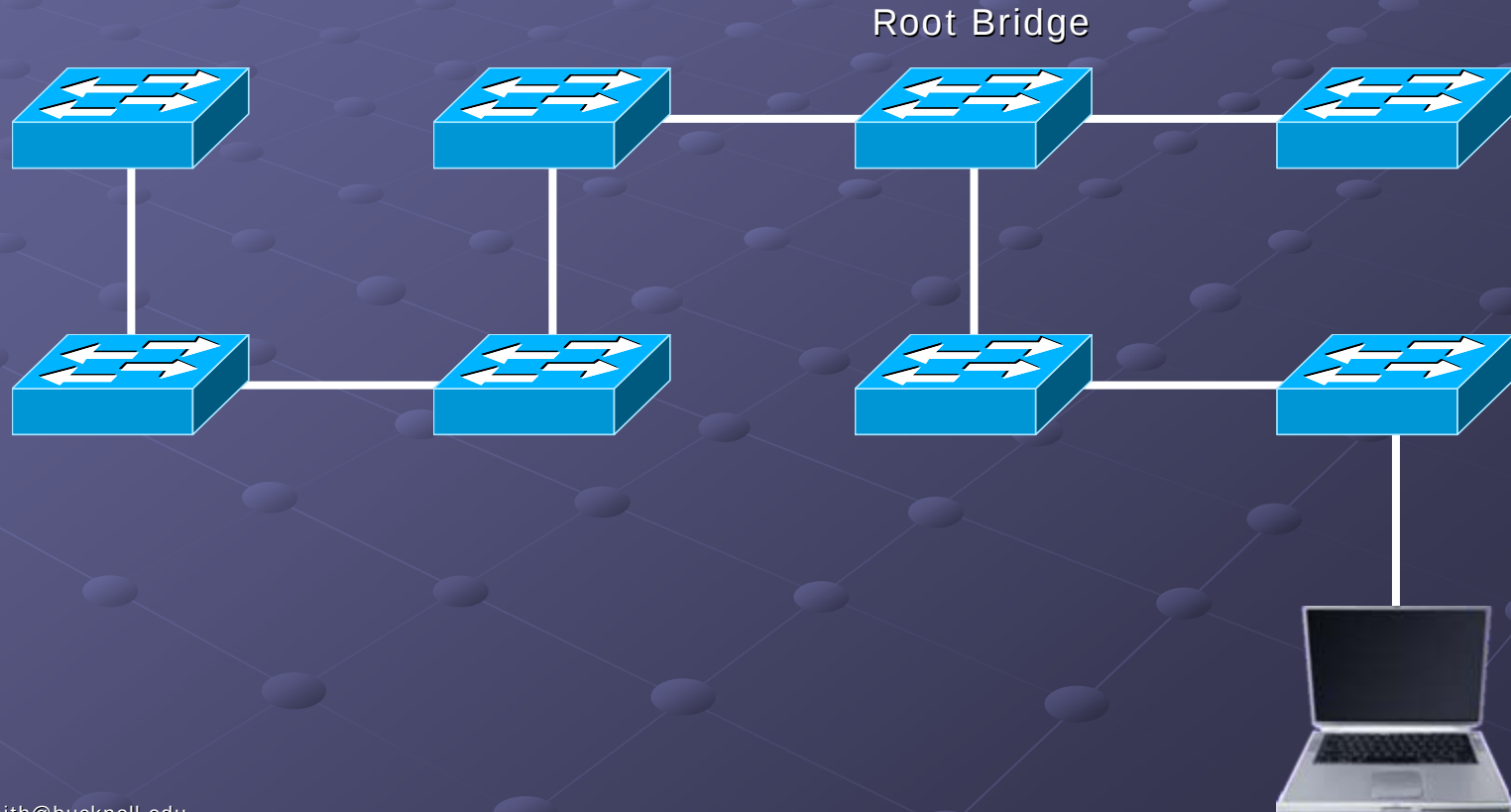
Spanning Tree

Physical Topology



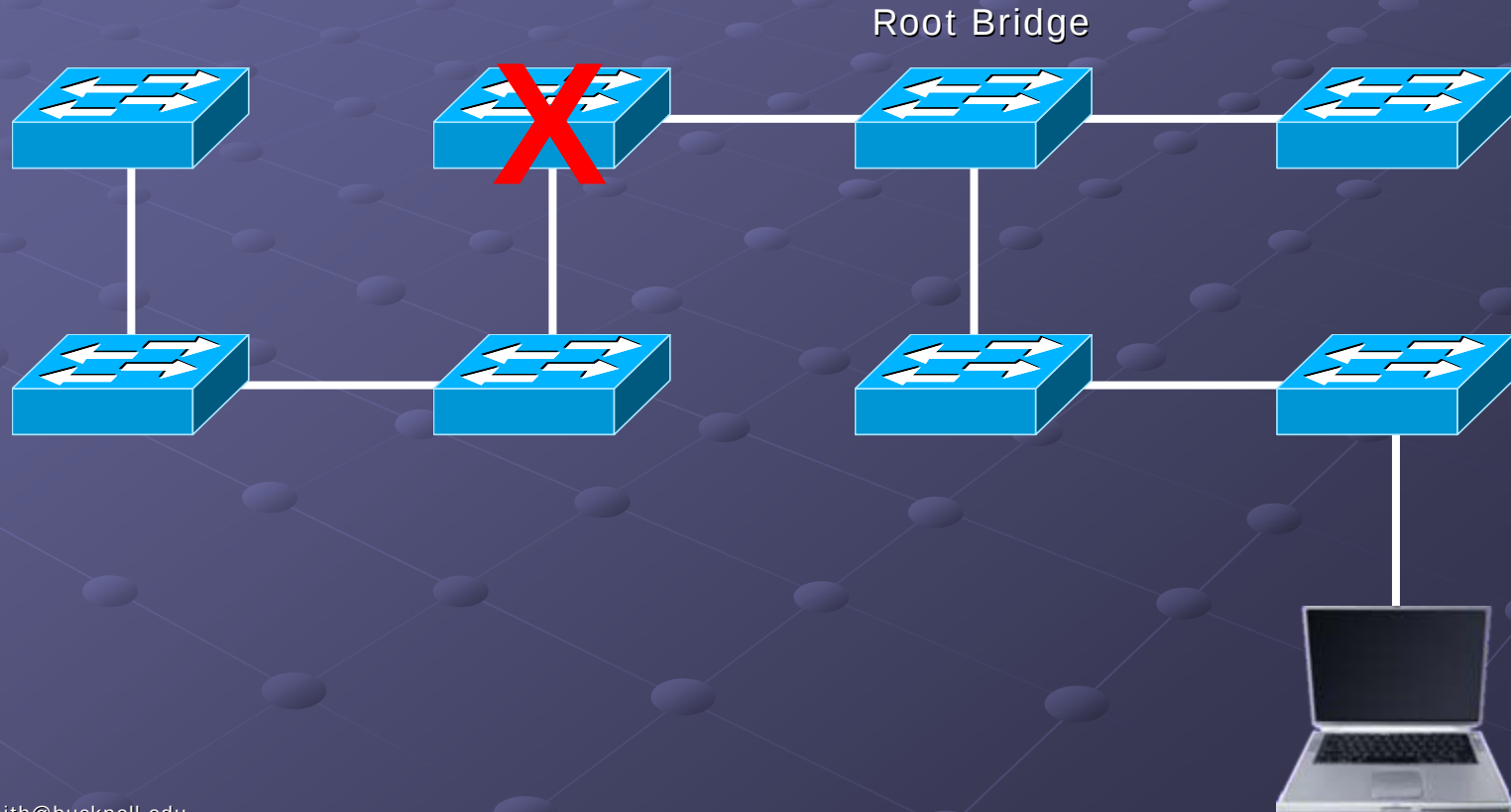
Spanning Tree

Logical Topology



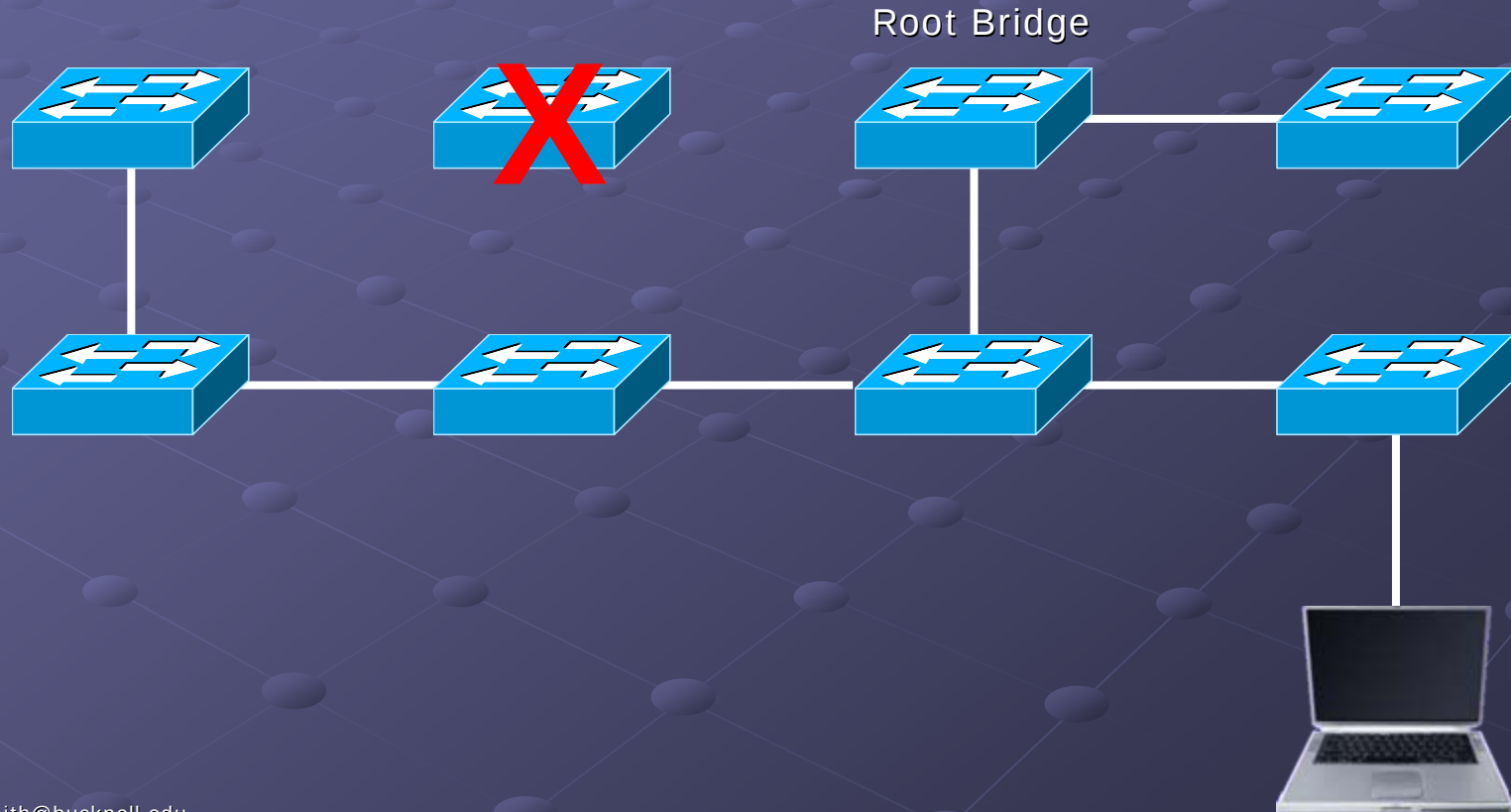
Spanning Tree

Switch or Link Failure



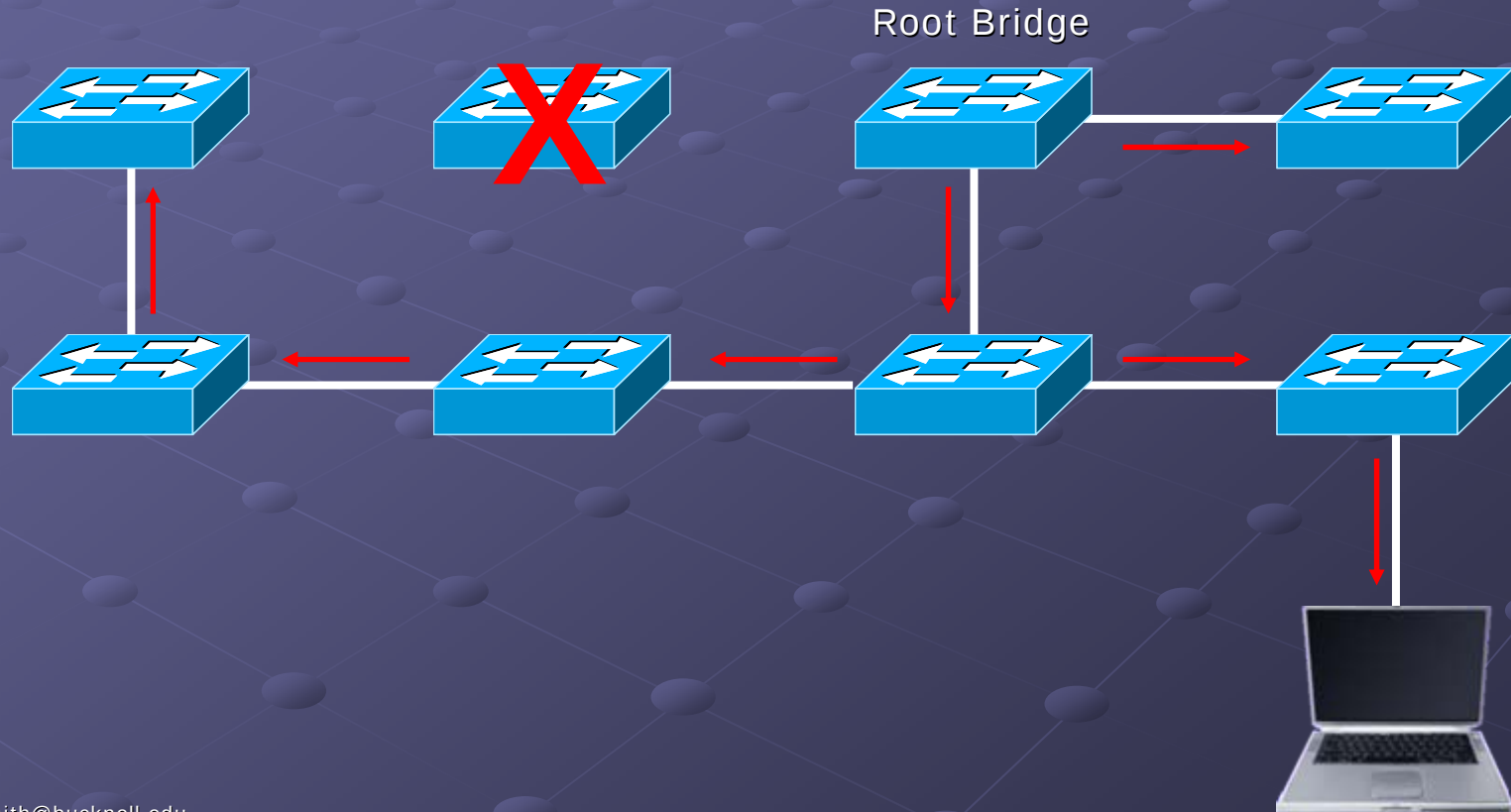
Spanning Tree

Switch or Link Failure



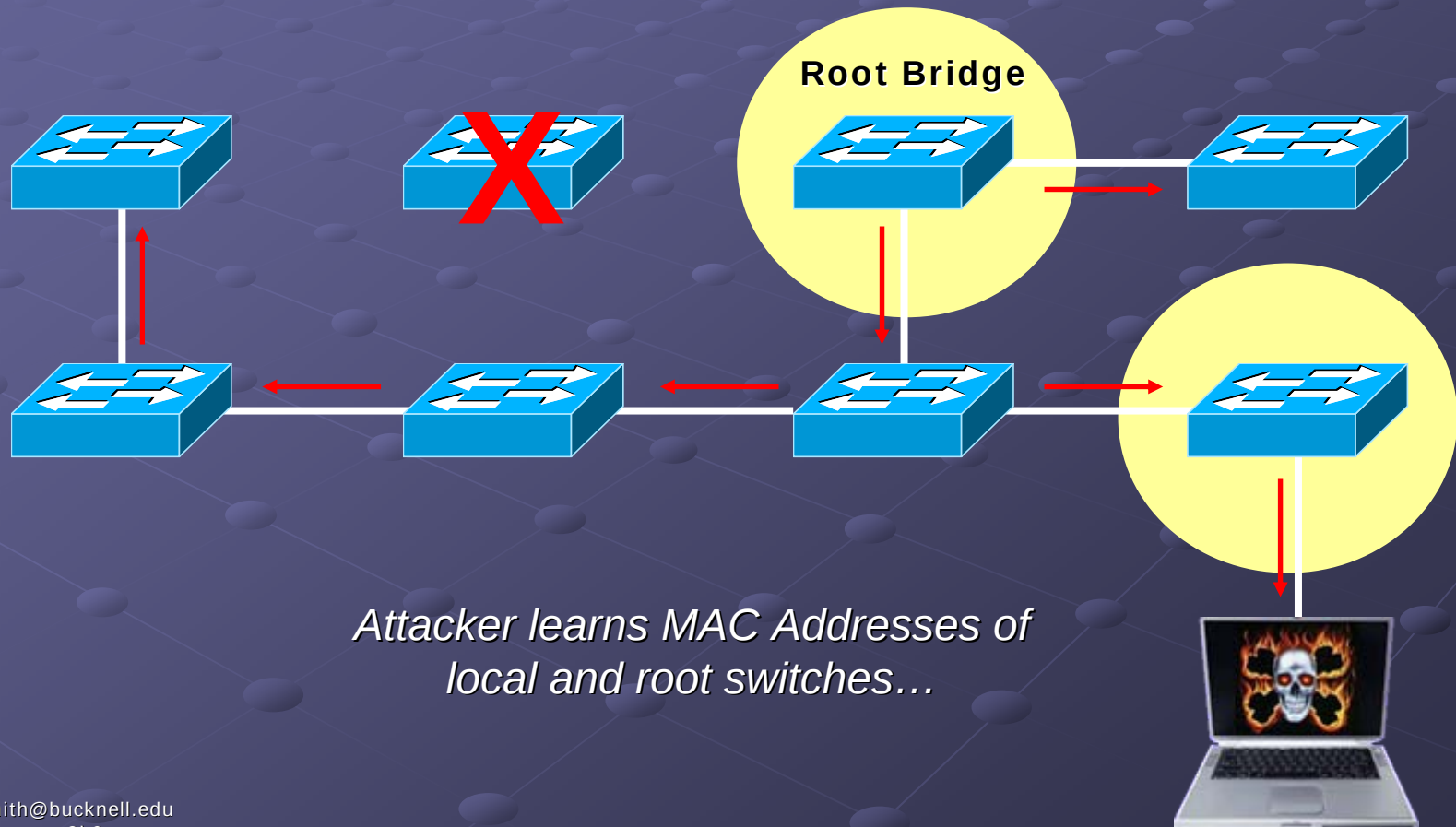
Spanning Tree

Bridge Protocol Data Units (BPDU)



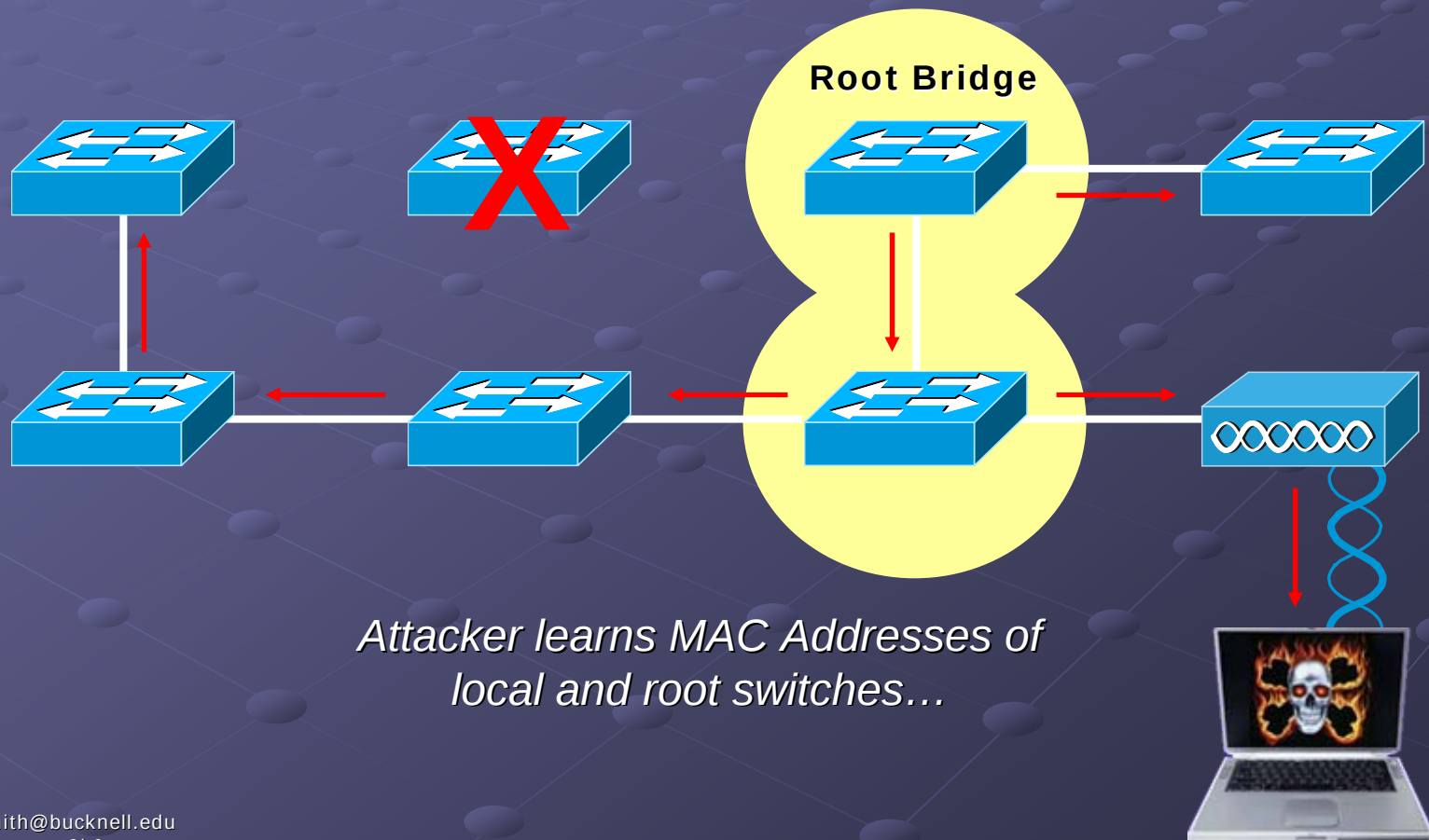
Spanning Tree

Bridge Protocol Data Units (BPDU)

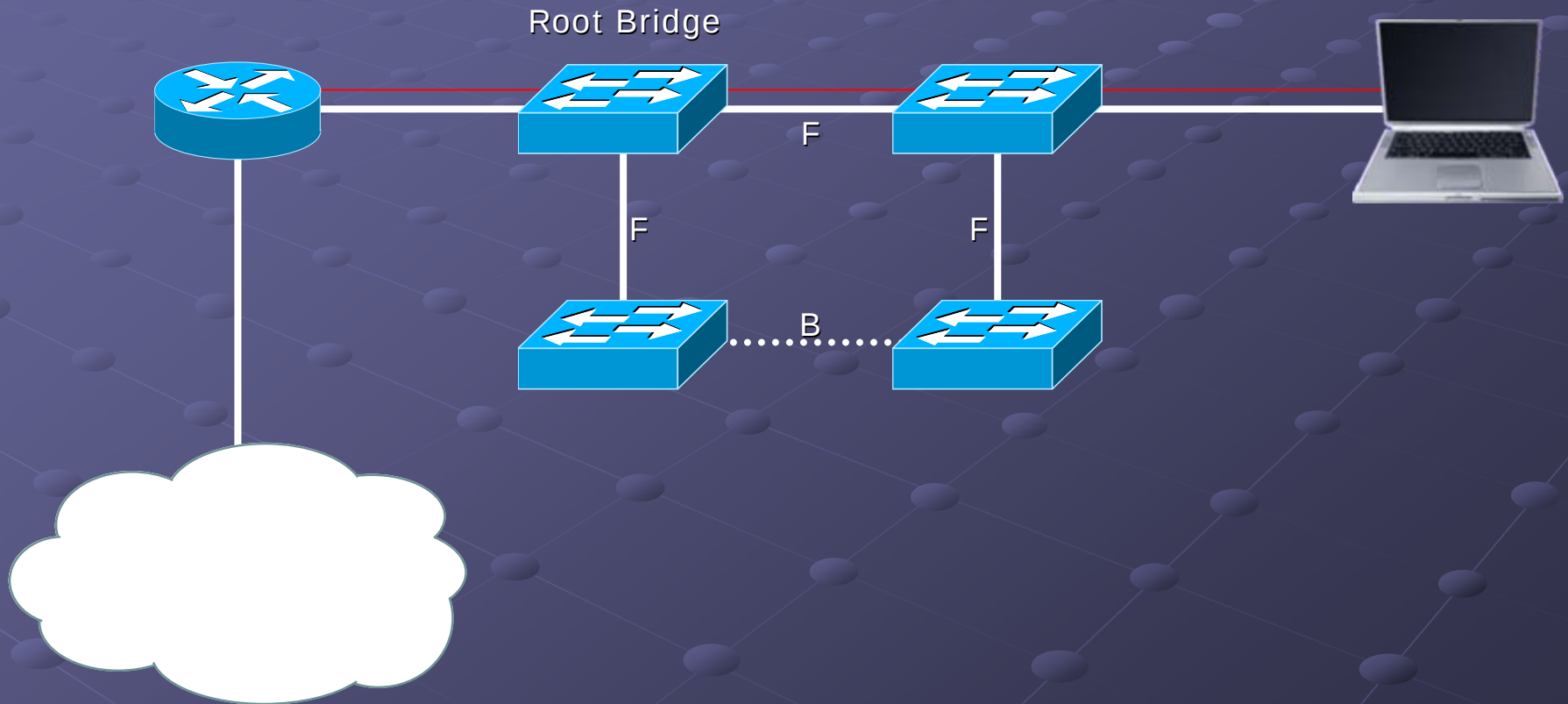


Spanning Tree

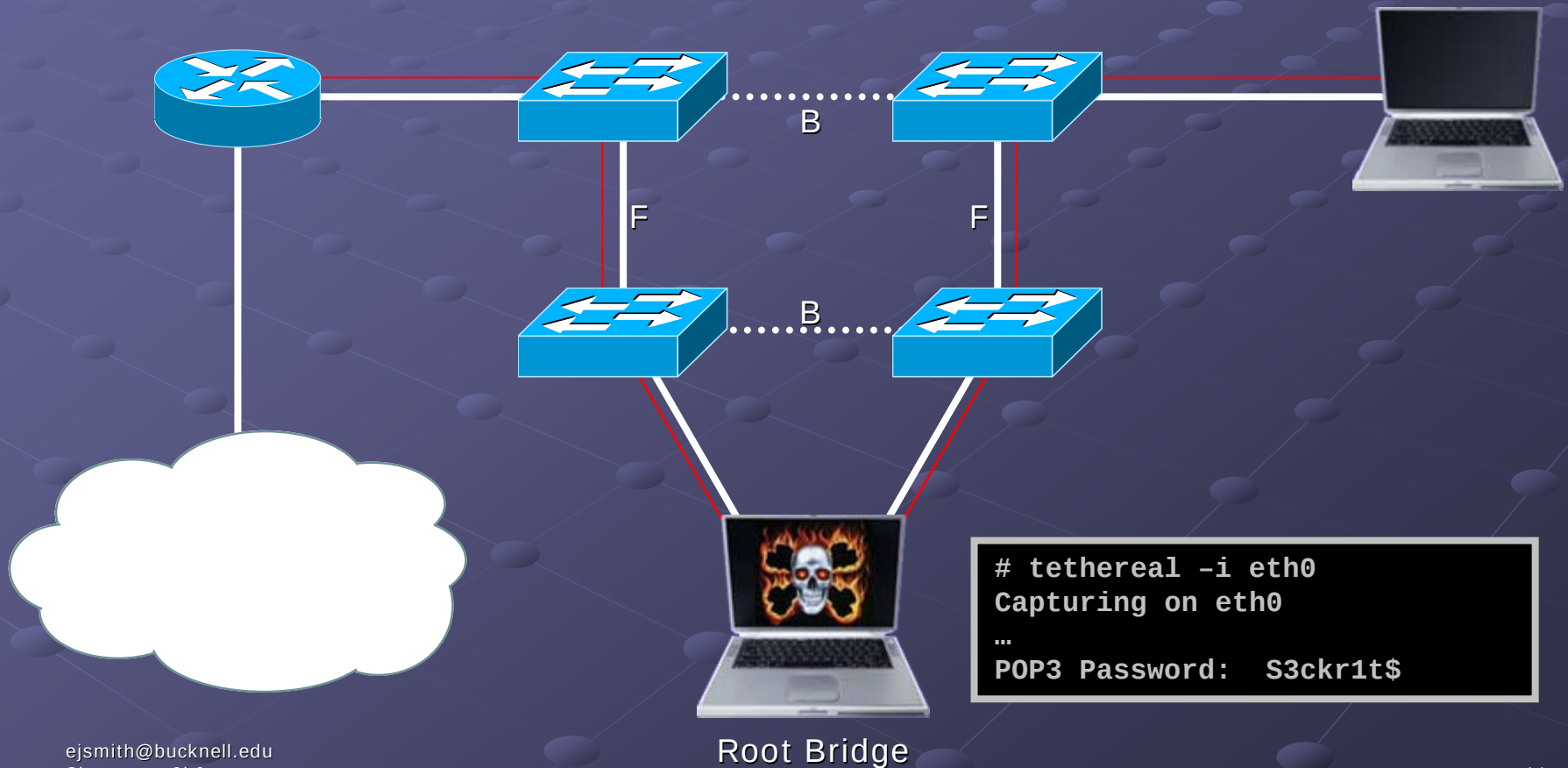
Bridge Protocol Data Units (BPDU)



Spanning Tree Attacks



Spanning Tree Attacks



Spanning Tree Countermeasures

1) No L2 redundancy? Don't Use STP

```
switch(config)# no spanning-tree vlan 1-4094
```

2) Disable STP per interface

```
interface fa0/1
  desc access port
  spanning-tree bpdufilter enable
  spanning-tree bpduguard enable
end
```

3) Use Root Guard to limit scope of STP topology changes

```
interface fa0/1
  desc access port
  spanning-tree guard root
```


Agenda

ARP

MAC Spoofing

Spanning Tree



Cisco Discovery Protocol (CDP)

Dynamic Trunking Protocol (DTP)

Broadcast Flooding

Putting it all Together

CDP

Cisco Discovery Protocol

Proprietary protocol used by Cisco devices to discover directly-connected neighbors

Uses: Network Administration, some routing protocols, autoconfigurations (VOIP phones)

Devices store neighbor information (device name, protocol addresses, capabilities, etc) in RAM

CDP

Cisco Discovery Protocol

```
Cat6K> (enable) sh cdp neighbors
```

```
* - indicates vlan mismatch.
```

```
# - indicates duplex mismatch.
```

Port	Device-ID	Port-ID	Platform
2/1	Engineering_3550_1ST	GigabitEthernet0/1	WS-C3550
2/2	Engineering_3550_2ND	GigabitEthernet0/1	WS-C3550
2/3	Engineering_3550_3RD	GigabitEthernet0/1	WS-C3550
2/4	Engineering_3550_4TH	GigabitEthernet0/1	WS-C3550

CDP

```
Cat6k> (enable) sh cdp neighbors 2/11 detail
Port (Our Port): 2/11
Device-ID: Engineering_Labs_3550
Device Addresses:
  IP Address: 172.16.4.24
Holdtime: 156 sec
Capabilities: SWITCH IGMP
Version:
  Cisco Internetwork Operating System Software
  IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.1(20)EA1a, RELEASE SOFTWARE
  (fc1)
  Copyright (c) 1986-2004 by cisco Systems, Inc.
  Compiled Mon 19-Apr-04 21:42 by yenanh
Platform: cisco WS-C3550-24-PWR
Port-ID (Port on Neighbors's Device): GigabitEthernet0/1
VTP Management Domain: Dist01
Native VLAN: unknown
Duplex: full
System Name: unknown
System Object ID: unknown
Management Addresses:
  IP Address: 172.16.4.24
Physical Location: unknown
```

CDP

More L2 Information Leakage



- Cisco Environment
- Model Number
- IOS Version
- Management IP Address
- Device Capabilities
- Native VLAN
- Partial network topology

CDP

Countermeasures

1) Disable CDP per device

```
Switch(config)#no cdp run
```

2) Disable CDP per port

```
interface FastEthernet0/24  
  desc access port  
  no cdp enable  
end
```

Agenda

ARP

MAC Spoofing

Spanning Tree

Cisco Discovery Protocol (CDP)

➔ Dynamic Trunking Protocol (DTP)

Broadcast Flooding

Putting it all Together

DTP

IOS Defaults encourage Dynamic Trunks

```
# sh run int fa0/24
```

```
interface FastEthernet0/24
  description default port setting on 3550 IOS 12.2.25
  switchport mode dynamic desirable
end
```

```
# sh int tru
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/24	desirable	n-isl	trunking	1

```
# sh dtp int fa0/24
```

```
3550_1_15#sh dtp int fa0/24
```

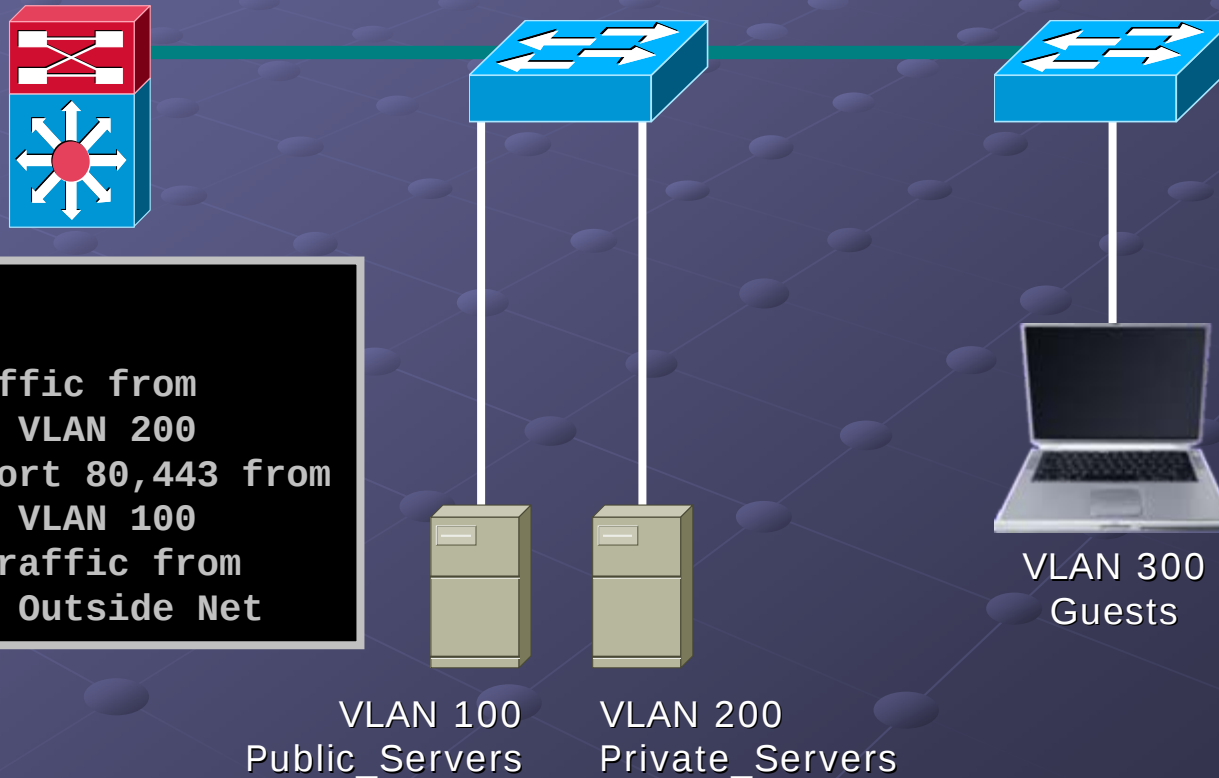
```
DTP information for FastEthernet0/24:
```

```
TOS/TAS/TNS:
```

```
TRUNK/DESIRABLE/TRUNK
```

DTP

Dynamic Trunking Protocol

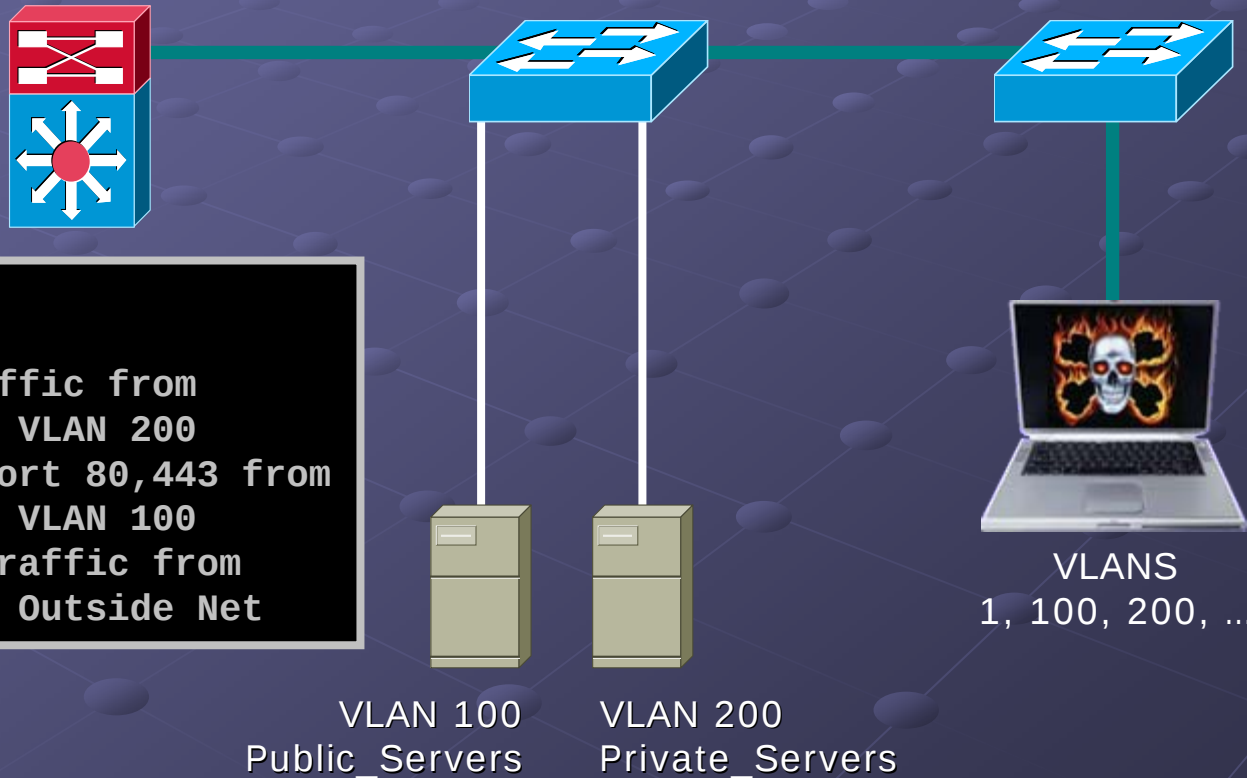


Router ACL:

```
Deny All Traffic from  
VLAN 300 to VLAN 200  
Permit TCP Port 80,443 from  
VLAN 300 to VLAN 100  
Permit All Traffic from  
VLAN 300 to Outside Net
```

DTP

Dynamic Trunking Protocol



DTP

Countermeasures

1) Disable DTP

```
interface fa0/24
  desc non-trunking port
  switchport access vlan 300
  switchport mode access
end
```

2) Disallow Sensitive VLANs on Dynamic Trunks

```
interface FastEthernet0/24
  desc allow trunking of specified vlans only
  switchport trunk allowed vlan 200,300
  switchport mode dynamic desirable
end
```

Agenda

ARP

MAC Spoofing

Spanning Tree

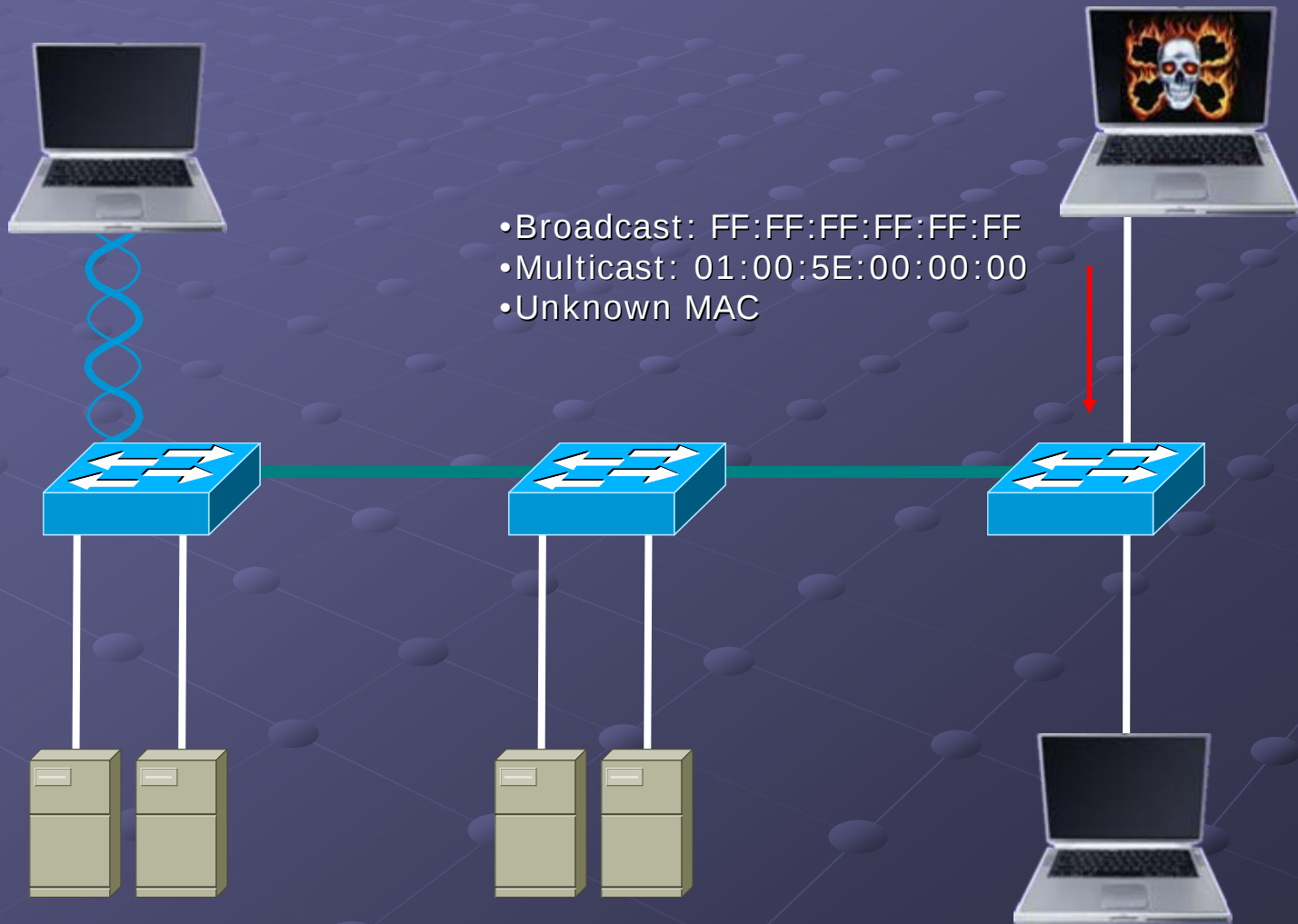
Cisco Discovery Protocol (CDP)

Dynamic Trunking Protocol (DTP)

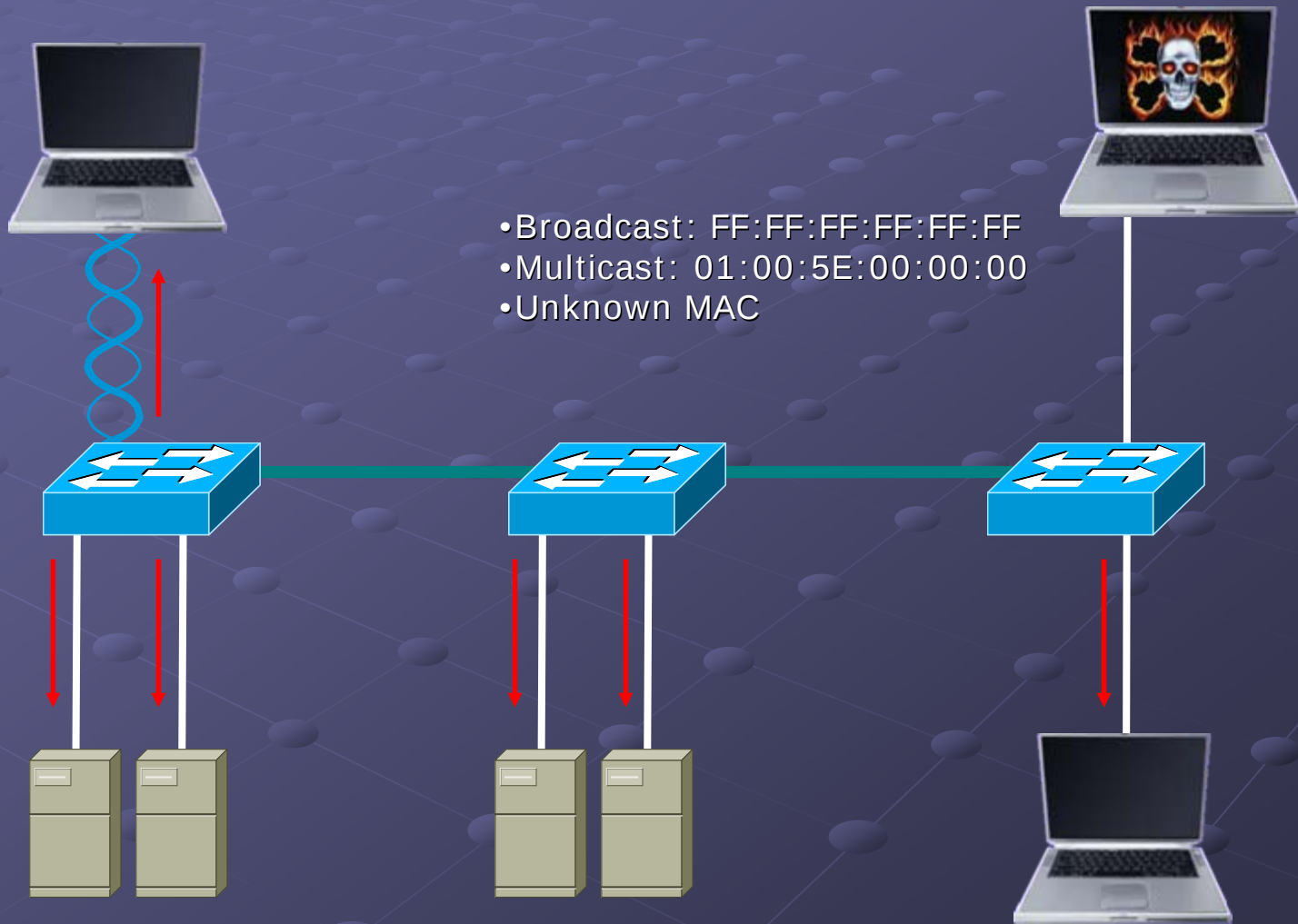
 Broadcast Flooding

Putting it all Together

Broadcast flooding



Broadcast flooding



Broadcast Flooding Countermeasures

1) Storm Control by Packet Rate

```
(config-if)# storm-control broadcast level pps 20 10  
(config-if)# storm-control unicast level pps 100 50  
(config-if)# storm-control multicast level pps 100 50
```

2) Storm Control by Bandwidth Ratio

```
(config-if)# storm-control broadcast level 1 0.5  
(config-if)# storm-control unicast level 50 40  
(config-if)# storm-control multicast level 1 0.5
```

Agenda

ARP

MAC Spoofing

Spanning Tree

Cisco Discovery Protocol (CDP)

Dynamic Trunking Protocol (DTP)

Broadcast Flooding



Putting it all Together

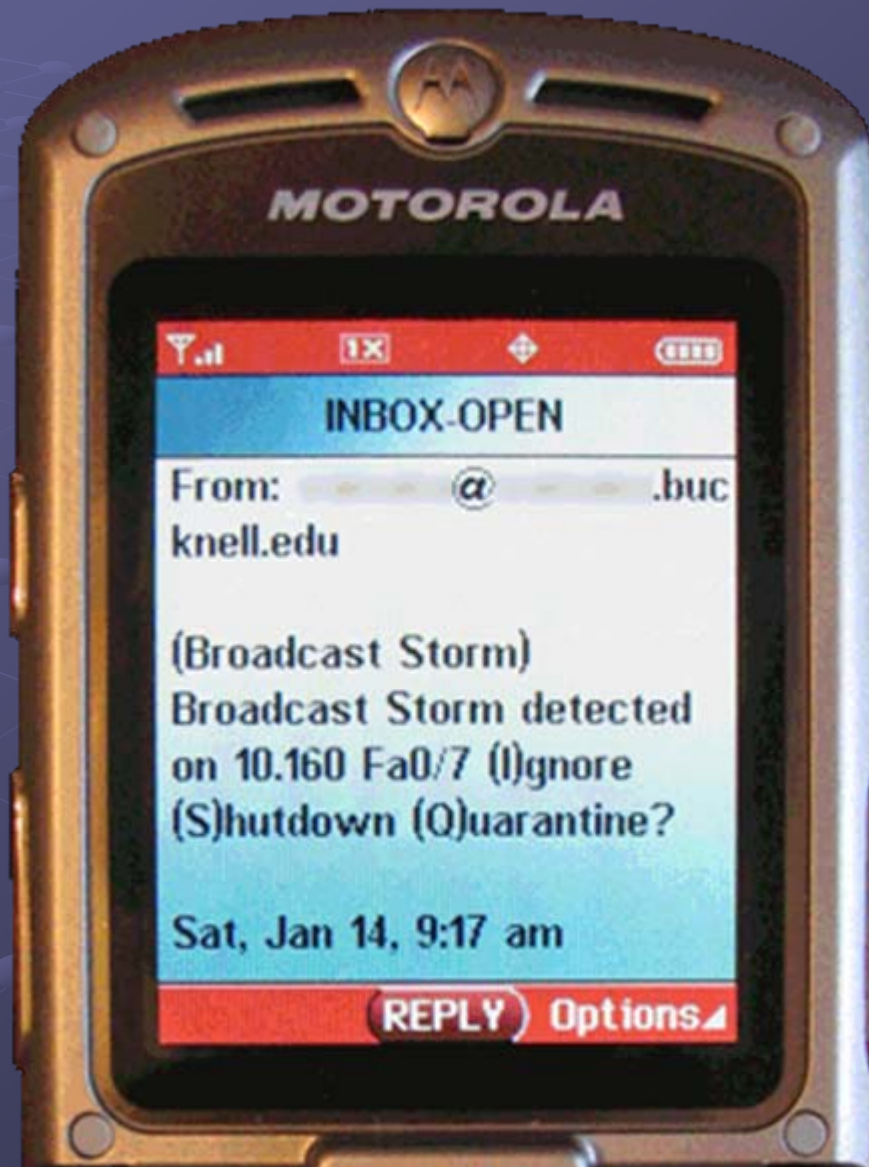
Better L2 Switch Configs

```
interface FastEthernet0/12
  description Somewhat more secure access port
  switchport mode access
  switchport access vlan 100
  switchport port-security
  switchport port-security maximum 5
  switchport port-security violation restrict
  storm-control broadcast level 1.00 0.50
  storm-control multicast level 1.00 0.50
  storm-control unicast level 50.00 40.00
  no cdp enable
  spanning-tree bpduguard enable
  spanning-tree guard root
  no keepalive
end
```

New Projects

L2KB:

Real-time
Layer 2
Incident
Response



New Projects

Wireless Killbot – Automatic Search-and-destroy of Rogue APs on the University Network



New Projects

Wireless Killbot Screen Shots

```
Welcome to  
KillBot 1.1  
Radio Scan Found  
9 network(s)  
Network 1 of 9  
SSID: linksys  
Encryption:  
Open *sigh*
```

```
Attempting to  
associate...  
Associated to  
0013.042f.34a4  
Lease Obtained  
192.168.1.100  
Rogue AP has  
been disabled :)
```

Recommended Reading

Network Security Architectures, Sean Convery
Cisco IOS Switch Security Configuration Guide, NSA

Acknowledgements

www.phenoelit.de/irpas

rude.sourceforge.net

Darren Cromer & Cisco PSIRT Team

Jeremy Powlus, Evil Graphics Overlord

Stephicus

Bill Barnes, PSKL / Bloomsburg University

Joel Bruno, PSKL

ShmooCon Staff & Goons

Bucknell University

Thanks for your attention!

Slides and code available at
www.presetkilllimit.us